S41447

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年9 月10 日 (10.09.2004)

PCT

(10) 国際公開番号
WO 2004/077754 A1

(51) 国際特許分類[7]: H04L 12/46, 12/28

(21) 国際出願番号: PCT/JP2004/000176

(22) 国際出願日: 2004 年1 月14 日 (14.01.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-6175 2003 年1 月14 日 (14.01.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): タン ペク ユー (TAN, Pek-Yew). チェン ホン (CHENG, Hong). タン チー ビン (TAN, Chee Bing).

(74) 代理人: 二瓶 正敬 (NIHEI, Masayuki); 〒1600022 東京都新宿区新宿２丁目８－８ とみん新宿ビル２Ｆ Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

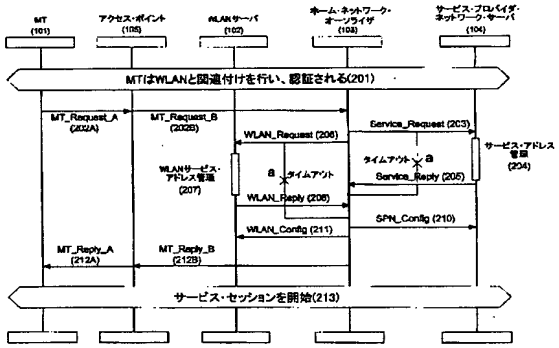
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: SERVICE IN WLAN INTER-WORKING, ADDRESS MANAGEMENT SYSTEM, AND METHOD

(54) 発明の名称: ＷＬＡＮ相互接続におけるサービス及びアドレス管理システム及び方法



(57) Abstract: There is provided a solution for managing mobile terminal address allocation in a WLAN inter-working. The mobile terminal acquires permission to access a service and an address and can establish a tunnel. Moreover, in the management process, protection is performed by an appropriate encryption and no special security setting procedure is required. Furthermore, there is provided a method for acquiring an address associated with a session by utilizing the service permission procedure. Even when a terminal accesses a plurality of sessions, it is possible to hold a plurality of addresses and the address management is integrated by the policy control mechanism. Thus, after an address modification, there is provided means for the terminal and its home network to constitute a WLAN. Moreover, by using a channel usable in the procedure, QoS or tunneling information is corrected according to a new status and provided.

[続葉有]

WO 2004/077754 A1

(57) 要約:

本発明によれば、ＷＬＡＮ相互接続における移動端末のアドレス割り当てを管理するための解決策が提供される。移動端末は、サービスへのアクセスの許可と共に、アドレスを取得してトンネルを設定することが可能となる。また、管理プロセスにおいては、特有の暗号化で保護され、特別なセキュリティの設定手続きが必要とされない。さらに、サービス許可手続きを利用して、セッションに関連するアドレスの取得を行うための方法が提供される。端末が複数のセッションにアクセスする場合でも、複数のアドレスを保持することができ、アドレス管理は、ポリシー・コントロール機構に統合される。これによって、アドレス変更後に、端末及びそのホーム・ネットワークがＷＬＡＮを構成するための手段が提供される。また、その手続きで利用可能なチャネルを使用して、ＱｏＳ、あるいはトネリング情報が、新たなステータスに応じて修正され、提供される。

明　細　書

ＷＬＡＮ相互接続におけるサービス及びアドレス管理システム及び方法

技術分野

本発明は、無線データ通信の分野に関する。また特に、本発明は、無線ＬＡＮ（ＷＬＡＮ）環境において、他のネットワークから訪れるモバイル・ユーザのためのアドレス管理に関し、ＷＬＡＮが、例えば、別の管理ドメイン内に存在し、他の無線技術を使用する３Ｇネットワークや ＷＬＡＮなどの公衆無線ネットワークとの相互接続（inter-networking）を行う際に使用可能なものである。また、本発明は、アドレス割り付け、構成、トンネリングの設定などのために、ＷＬＡＮ及び相互接続ネットワーク（inter-worked network）に加えて、移動端末によって利用可能であり、その結果、移動端末はＷＬＡＮにおいて加入したサービスにアクセス可能となる。

背景技術

ＷＬＡＮ相互接続（WLAN inter-working）では、端末が加入したすべてのサービスにアクセスすることができるように、端末はアドレス付けが可能（addressable）でな必要がある。サービスがＩＰを通じて伝送される場合、端末は、あるＩＰアドレスに関連付けられているはずである。モバイルの世界では、端末の接続点が頻繁に変わり、端末があるアクティブなサービス・セッションの間に、いくつかのドメインを渡り歩くことが十分に起こり得る。この端末の移動性の要件を満たすために、アドレス管理のメカニズムには、端末が接続点を変更するごとに、端末のアドレスを構成（configure）し更新することが要求される。

モバイルＩＰは、インターネット技術検討委員会（ＩＥＴＦ）で公開されている標準化技術であり（非特許文献１）（非特許文献２）、移動端末のためのアドレス管理とトラフィックのルーティングに対する解決策を提供する。この技術によって、様々なＩＰネットワーク内を動き回る場合に、ユーザは、同一のアドレスを使用しながら位置特定可能な状態（reachable）となる。移動性がＩＰレベルで管理されているので、モバイルＩＰは、基礎となるリンク層の技術に束縛されず、３Ｇのセルラ・ネットワーク、又は無線ＬＡＮ（例えば、８０２．１１のネットワーク）内の端末に対して、同一のプロトコル・スタックの適用が可能となる。例えば、ＷＬＡＮと３Ｇのセルラ・ネットワークとの相互接続などのアクセス技術の融合において、この種の調和したレベルの解決策が、特に有用である。モバイルＩＰでは、ＩＰ接続によってアドレス管理が行われ、ＩＰ接続が利用可能でない場合には、アドレス管理が不可能となる。また、さらに、モバイルＩＰでは、端末が、ホーム・アドレスを有し、かつ、そのホーム・エージェントを知っている必要がある。こうした要件は、例えば、端末が最初にフォーリンＷＬＡＮで動作を開始する場合など、相互接続の動作過程では満たされないかもしれない。

また、モバイルＩＰｖ６のドラフトでは、移動ノード（mobile node）のホーム・アドレスのセッティング方法が導入されている（非特許文献２）。端末は、例えば、ＤＨＣＰｖ６（非特許文献３）を使って、まず、気付アドレス（Care of address）を最初に生成し、このアドレスを使用して、最終的なホーム・アドレスを設定するホーム・ネットワークとの通信を行う。しかし、ＷＬＡＮから得られた気付アドレスを使用した場合には、移動ノードのホーム・ネットワークは必ずしも位置特定可能な状態とはならないので、ＷＬＡＮ相互接続においては、動作が不可能となる。さらに、複数回のやり取りを行うコンフィギュレーション処

理は、時間を消費するものであり、ユーザの期待に沿うものとはならない。

また、ダイアメータ・モバイルＩＰｖ６の適用（非特許文献４）によって、ＡＡＡの構成に基づいて、モバイルＩＰｖ６のアドレス管理のための解決策が示されている。この解決策では、ＡＡＡサーバと移動先及びホーム・ネットワークのクライアントが、アドレス更新及びエージェント発見を実行することが利用されている。そのメカニズムでは、移動ノードは、例えば、ルータ・アドバタイズメント・メッセージを聞くことができるなど、メッセージ交換用のローカルＩＰ接続を有することが要求されるが、フォーリン・ドメインのローカル・ポリシーによって、必ずしも可能であるとは限らない。さらに、この機構は、アドレスが移動端末のホーム・ドメインに属する状況でのみ提供されるものである。ＷＬＡＮ相互接続では、端末がアクセスしているサービスに依存する別のドメインからのアドレスを端末が使用することになり、このアドレスは端末のサービス・リクエストの情報を持たないので、この機構はＷＬＡＮ相互接続をサポートすることはできない。この機構は、モバイルＩＰｖ６環境のために設計されており、したがって、モバイルＩＰスタックのない端末では動作不可能である。

さらに、３ＧＰＰによって解決策、端末のアドレシングとトンネリングとを管理するためのＧＴＰ（非特許文献５）が提供されている。ＧＴＰは、コントロール用のＧＴＰ－Ｃ、及び、ユーザ・データのトラフィック用のＧＴＰ－Ｕの２つのパートを有している。ＧＴＰは、ＵＤＰ上で動作し、ＵＤＰパケット中のユーザ・データをカプセル化する。このＧＴＰは、ＧＰＲＳ（非特許文献６）ネットワーク用に設計されており、例えば、ＧＧＳＮ、ＳＧＳＮノードなどのＧＰＲＳネットワークの特徴に非常に依存しており、単純な無線アクセス・ネットワーク（例えば、

ＷＬＡＮ）への適用は困難である。

非特許文献１　「IP mobility support for IPv4」
http://www.ietf.org/rfc/rfc3344.txt

非特許文献２　「Mobility support in IPv6」
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-19.txt

非特許文献３　「Dynamic Host Configuration Protocol for IPv6 (DHCPv6)」
http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-28.txt

非特許文献４　「Diameter Mobile IPv6 Application」
http://www.ietf.org/internet-drafts/draft-le-aaa-diameter-mobileipv6-02.txt

非特許文献５　「GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (Release 5)」　3GPP TS 29.060 V5.3.0 (2002-09)
ftp://ftp.3gpp.org/Specs/archive/29_series/

非特許文献６　「General Packet Radio Service (GPRS); Service description; Stage 2 (Release 5)」　3GPP TS 23.060 V5.2.0 (2002-06)
ftp://ftp.3gpp.org/Specs/archive/23_series/

非特許文献７　「IP Multimedia Subsystem (IMS); Stage 2 (Release 5)」　3GPP TS 23.228 V5.6.0 (2002-09)
ftp://ftp.3gpp.org/Specs/archive/23_series/

非特許文献８　「Diameter Base Protocol」
http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-15.txt

非特許文献９　「PPP Extensible Authentication Protocol (EAP)」
http://www.ietf.org/rfc/rfc2284.txt

非特許文献１０　3GPP project　http://www.3gpp.org

非特許文献１１　3GPP2 project　http://www.3gpp2.org

非特許文献１２　「The Network Access Identifier」
http://www.ietf.org/rfc/rfc2486.txt
非特許文献１３　「Numbering, addressing and identification (Release 5)」　3GPP TS 23.003 V5.3.0 (2002-06)
ftp://ftp.3gpp.org/Sepcs/archive/23_series/
非特許文献１４　「Port-Based Network Access Control」　IEEE Std 802.1X-2001　http://standards.ieee.org/getieee802/
非特許文献１５　「Diameter Extensible Authentication Protocol (EAP) Application」
http://www.ietf.org/internet-drafts/draft-ietf-aaa-eap-00.txt
非特許文献１６　「Diameter NASREQ Application」
http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-09.txt
非特許文献１７　「IPv6 Stateless Address Autoconfiguration」
http://www.ietf.org/rfc/rfc2462.txt

通常、ＷＬＡＮ及び相互接続ネットワークは、異なる管理ドメインに存在している。これは、アドレス空間が別々に管理されていることを意味している。したがって、移動端末が、そのホーム・ネットワークとは異なるドメインのＷＬＡＮに移動した場合、端末への連続的なサービス配送を保証するために、何らかのアドレス構成を実行しなければならない。このアドレス構成には、例えば、ＩＰアドレス割り付け、アドレス登録、トンネリングの設定なども含まれている。

ＷＬＡＮを通じて端末に任意のサービスが配送されるようにするためには、アドレスの限定が行われる。例えば、ＷＬＡＮから３Ｇネットワーク内のＩＭＳ（非特許文献７）サービスにアクセスするためには、端末は、ＩＭＳを提供するネットワークに属するアドレスを有する必要が

あり、結果的に、異なるサービスへの並列のアクセスを行う移動端末は、複数のＩＰアドレスが割り当てられるよう要求される。

ＷＬＡＮでは、認証及びその許可が与えられる前に、端末が、例えば、通常のデータ・パケットを送受信するなど、いかなるリソースを使用することも許されていない。例えばＭＩＰｖ６の中で示唆されるような通常の機構では、許可処理の成功後にのみアドレスの構成が行われるが、この種のアプローチは時間がかかり、いくつかのサービスにおける要件を満たすことができない。この許可処理の前にアドレス構成を行うためには、アドレス構成に関連した情報がアクセス・コントロール・メッセージに統合される必要がある。また、アドレス管理は通常、ユーザの加入情報に基づいており、移動端末のホーム・ネットワークによって管理される必要がある。しかし、任意の外部サービスにおいては、ホーム・ネットワーク以外のドメインから、アドレスが割り当てられる必要がある。この場合、ホーム・ネットワークが、アドレス割り当てやそのドメインが有する他の情報に関するやり取りを行えるメカニズムが必要となる。

また、端末がアドレスを変更する場合、その端末に関連した終端点間（エンド・トゥー・エンド）ＱｏＳが影響を受けることになる。例えば、もしアドレスが変わった場合には、送信元アドレス又は送信先アドレスの情報に基づくトラフィック・フィルタは、流れ（フロー）を正確に分類することは不可能となる。ファイア・ウォールや他のトラフィック・コントロール機能を実施するＷＬＡＮについては、さらに、端末の新しいアドレスが示される必要があり、さもないと、トラフィックが妨げられるか、又は、中断されることとなる。

発明の開示

端末がＷＬＡＮに入った場合、端末は、リソースへのアクセスを行うために、認証処理及び許可処理を完結しなければならない。本発明では、アクセス・コントロール・メカニズムに統合されるアドレス管理への解決策が示される。この統合によって、アクセスの許可と同時に、端末のアドレスの割り当てが行われることが可能となる。また、端末は、アクセス・コントロール・メカニズムを再利用して拡張するので、新しいプロトコルを実施する必要はない。アドレスの構成処理は、アクセス・コントロール処理の固有の暗号化及び保護によって守られ、したがって、特別なセキュリティの設定を必要としない。

また、本発明は、さらに、端末のホーム・ネットワークが端末のサービスを提供するネットワークとアドレス管理の取り決めを行うための手段を提供する。この種のやり取りは、バック・エンド・プロセスであり、移動端末とＷＬＡＮには明らかなもの（transparent）であり、その取り決めの結果は、サービス許可処理を利用して、ＷＬＡＮ及び移動端末に送られることとなる。

また、並列のアクセス・セッションが同一の端末に存在する場合には、複数のアドレスが要求されることとなる。本発明では、きめ細かいサービス許可処理を使用して、端末がセッションに関連するアドレスを取得するための方法が提供される。各セッションは、関連付けられたアドレスを使用して、新しいアドレスへの移行が行われる。

また、アドレス管理は、ポリシー・コントロール・メカニズムにも統合される。ポリシー・コントロールは、アドレスが変わった後、必要な場合には、端末及びそのホーム・ネットワークにＷＬＡＮを構成するための手段を提供する。ＱｏＳ、又は、トンネリングの情報は、既存のポリシー・コントロール処理で利用可能なチャンネルを使用した新しいステータスに従って、修正され、供給される。これによって、ローミング

時間内に、アドレスのスムーズな移行を達成することが可能となり、ＱｏＳの中断を最小限に抑えることが可能となる。

図面の簡単な説明

図１は、本発明のＷＬＡＮ相互接続における移動端末のアドレスの割り当て、トンネルの設定、サービスの取り決めの管理に使用されるネットワーク構成の一例を示すブロック図、

図２は、図１に示される構成で使用される、端末のアドレスの割り当て、トンネルの設定、サービスの取り決めのためのメッセージ・シーケンスの一例を示すシーケンス・チャート、

図３は、図２に示されるメッセージ交換で移動端末によって使用されるメッセージの構成の一実施例を示すデータ構造図、

図４は、アドレス割り当て要求のために移動端末によって利用されるフォーマットの一例を示すデータ構造図、

図５は、ＷＬＡＮ相互接続における移動端末のアドレス割り当て、トンネルの設定、サービスの取り決めのための図１で示されるフレームワークにおけるホーム・ネットワーク・オーソライザの一実施例を示す状態遷移図、

図６は、ホーム・ネットワーク・オーソライザで要求メッセージの処理手続きを行うために使用され得るフローチャートの一例を示すフローチャート、

図７は、サービス・プロバイダ・ネットワーク・サーバと移動端末のサービスの詳細、アドレス割り当て、トンネル設定の取り決めを行うために、ホーム・ネットワーク・オーソライザによって使用されるメッセージの構造の一実施例を示すデータ構造図、

図８は、ＷＬＡＮサーバと移動端末のサービスの詳細、アドレス割り

当て、トンネル設定の取り決めを行うために、ホーム・ネットワーク・オーソライザによって使用されるメッセージの構造の一実施例を示すデータ構造図、

図９は、ホーム・ネットワーク・ドメイン内のポリシー・サーバの移動端末の状態に関する更新を行うために、ホーム・ネットワーク・オーソライザによって使用されるメッセージの構造の一実施例を示すデータ構造図である。

発明を実施するための最良の形態

本発明は、ＷＬＡＮが他のネットワークと相互接続（inter-work）するために使用されるものである。相互接続されたネットワークとしては、別のＷＬＡＮ又は公衆セルラ・ネットワークが可能であり、どちらの場合においても、容易に、本発明を適用することが可能である。また、本発明は、アドレス管理や、アドレスの遷移（つまり、モビリティ・コントロール）に関連したサービス提供を行うことを目的として使用されるものである。

ここで提案される機構（スキーム）を適用する場合には、特別なインターフェースやプロトコルを実施する必要はない。この機構は、既存のアクセス・コントロール・メカニズムを再利用し、必要な機能性を支援するために、その属性のうちのいくつかを拡張する。アドレス割り付けでは、その修正がサービス許可手続きに統合される。許可手続きが、認証から得られた信頼によって暗号化され保護されるので、アドレス情報も同一のセキュリティ・レベルで保護され、許可情報の一部として示されて、通常の許可情報と同一の方法で転送可能となる。例えば、ＡＶＰに特有の許可としてダイアメータ（非特許文献８）に含まれたり、ＥＡＰ方法による許可が利用可能な場合には、ＥＡＰ（非特許文献９）の属

性として含まれたりすることが可能である。

端末がＷＬＡＮに入った場合には、サービスを利用することが認められる前に、認証及び許可が行われる。許可手続きでは、端末が、アクセスしようとするサービスを要求し、この情報はＷＬＡＮを通じて端末のホーム・ネットワークに渡される。端末のホーム・ネットワークは、ユーザの加入者プロフィールに基づいてサービスを許可すべきか否かを決定する。さらに、要求されたサービスに応じて、端末のホーム・ネットワークは、サービスに使用されるアドレスを決定する。例えば、ＩＭＳサービスについては、アドレスはＩＭＳアドレス空間から割り当てられる必要があり、一方、ローカルＷＬＡＮサービスについては、ローカルで取得されたアドレスで十分である。また、さらに、アドレス管理に関連するトンネリングの情報の確認が行われる。

アドレス情報は許可情報に含まれ、許可成功メッセージと共に送られる。この情報の一部は、ＷＬＡＮに送られ、一部は、通常の許可手続きと同様、端末に送られる。例えば、端末が端末自体のアドレス構成を行えるようにするために、アドレスが端末に送られる必要がある。また、もしネットワーク・トンネリングが必要な場合には、ＷＬＡＮによって、トンネリングの情報が使用される。

また、アドレスの変更が必要な場合には、サービス許可の詳細な手続きを行わずに、迅速な更新を行うために、再許可手続きを利用することが可能である。

また、端末がサービスへのアクセスを開始した場合に、ポリシー・コントロールが開始される。アドレス情報は、端末のホーム・ネットワークのポリシー・サーバによって利用可能となり、その後、ポリシー・サーバは、ポリシー決定をアドレス情報に基づいて行うことが可能となる。また、アドレスの変更時には、ポリシー・サーバに対して、対応するポ

リシーを更新するよう通知が行われ、その結果、ＱｏＳ及びサービス提供が保証される。

発明の理解を支援するため、次の定義が使用される。

「ＷＬＡＮ」は、無線のローカル・エリア・ネットワークを指すものであり、無線技術を通じて移動端末にＬＡＮサービスを提供するための任意の数の装置を含むものである。

「３Ｇネットワーク」は第３世代の公衆アクセス・ネットワークを指すものであり、例えば、３ＧＰＰ（非特許文献１０）や３ＧＰＰ２（非特許文献１１）によって定義されるシステムである。

「移動端末」は、無線技術によってＷＬＡＮ及び他のネットワークによって提供されるサービスへのアクセスに使用される装置を指すものである。

「ホーム・ネットワーク」は、移動端末（ＭＴ）のサービス加入情報が格納されているネットワークを指すものであり、相互接続のシナリオでは、ＭＴが最初に加入したネットワーク、又は、ＭＴの加入情報に完全にアクセスすることが許可されている訪問先のネットワークである。

「サービス・プロバイダ・ネットワーク」は、ＭＴが要求したサービスが提供されるネットワークを指すものであり、例えば、ホーム・ネットワーク、ＷＬＡＮ、外部ネットワークなど、任意のネットワークが可能である。

「ネットワーク・エレメント」は、情報処理を実行することが可能なネットワーク内で機能している任意の装置を指すものである。

「ポリシー・サーバ」は、ネットワーク・ドメインのポリシー・コントロール機能を実行するネットワーク・エレメントを指すものである。ポリシー・コントロール機能は、例えば、ローカルのリソース配分、パケット・フィルタの更新、ルーティングの更新などを含んでいる。

「エア・インターフェース」は、移動端末がＷＬＡＮにアクセスするための任意の無線アクセス技術を指すものである。

「ストリーム」は、ある属性を共通に持っているネットワーク内で転送されるパケットの集まりである。

「トラフィック」は、ネットワーク内で転送されるストリームの集まりである。

「フロー」は、データ・パス、及び、ストリームを伝送するために使用されるデータ・パスに必要とされるネットワーク・リソースを指すものである。

「ＱｏＳ」は、データ・ストリーム又はトラフィックのサービス品質（Quality of Service）の用語を指すものである。

「メッセージ」は、相互接続をコントロールする目的で、ネットワーク・エレメント間で交換される情報を指すものである。

「オペレーション・シーケンス」は、相互接続コントロールのために、任意のネットワーク・エレメント間での一連のメッセージ交換を指すものである。

「上位レイヤ」は、現在のエンティティの上に存在し、現在のエンティティから渡されたパケットを処理するすべてのエンティティを指すものである。

「クライアントに基づくトンネル」は、トンネルの終端点のうちの１つが移動端末であるトンネリング機構を指すものである。

「ネットワークに基づくトンネル」は、トンネルの終端点が移動端末以外のネットワーク・エレメントに存在するトンネリング機構を指すものである。

以下の記述では、本発明を完全に理解するための説明において、具体的な数、時間、構造、プロトコルの名前、その他のパラメータが使用さ

れるが、このような具体的な詳述がなくても、本発明の実施が可能なことは当業者にとって明白である。また、よく知られた構成要素やモジュールに関しては、本発明を不必要に不明瞭なものとしないようブロック図で示されている。

端末が高度な移動性を有するという特性により、モビリティ・コントロールは、ＷＬＡＮ相互接続における最も顕著な問題のうちの１つである。端末が移動する場合、端末は、接続点に局所的（ローカル）でないアドレスを使用するよう要請されている。例えば、ＷＬＡＮに入り込んだ３Ｇ端末に関しては、そのホーム・ネットワークのサービス（例えば、ＩＭＳサービス）にアクセスするためには、３Ｇドメインのアドレスが必要とされる。端末が、３Ｇネットワーク内にあるサービスを開始した場合、アドレスは、例えば、ＧＰＲＳサービス（非特許文献６）などの３Ｇのスキームに従って割り当てられ、このアドレスは、端末の３Ｇセルラ・インターフェースに関連付けられる。また、端末がＷＬＡＮドメインに入る場合には、高いスループットを実現することができるので、そのＷＬＡＮインターフェースを使用して通信することが望まれる。例えば、２重のインターフェース（ＧＰＲＳ及びＩＥＥＥ８０２．１１）を備えたＰＤＡは、道路上ではＧＰＲＳインターフェースを使用し、ホット・スポット内ではＩＥＥＥ８０２．１１インターフェースを使用することが望まれる。端末がＷＬＡＮインターフェースを使用して３Ｇサービスにアクセスする場合には、端末は、３Ｇインターフェースから得られたものと同一のアドレスを使用し続ける必要がある。そうでなければ、端末はサービス中断に直面し、セッションを再度初期設定しなければならず、これは、ユーザにとって望ましいことではない。また、使用中のアドレスはＷＬＡＮに局所的ではないので、トンネルは、端末からサービス・プロバイダ・ネットワークまで設定されなくてはならない。

図１には、アドレス割り付けとトンネルのセット・アップのための本発明の実施例が示されている。なお、混乱を避けるため、シグナリングに参加するネットワーク・エンティティのみが図示されている。

移動端末（１０１）はネットワークからあるサービスを要求するエンティティである。実際には、例えば、Bluetoothリンクによってラップトップ・コンピュータに接続されたハンドセットなどのように、いくつかのエンティティを有することが可能であるが、単純化のため、図１には１つのセットとして描かれている。ＷＬＡＮ機能（WLAN function）（１００１）内において、アクセス・ポイント（１０５）は、移動端末（１０１）に対してＷＬＡＮアクセスを提供するエンティティである。移動端末（１０１）がＷＬＡＮサービスを利用する許可が与えられるまで、アクセス・ポイント（１０５）は、移動端末（１０１）からのデータ・トラフィックをすべて遮断するが、ある特定のデータ・パケットのみを許可するコントロール・チャンネルが、アクセス・コントロール・シグナリングを行うために開いた状態（open）となる。移動端末（１０１）は、無線リンク（１０１１）を通じてアクセス・ポイント（１０５）と通信を行う。このリンクとして、例えば、ＩＥＥＥ８０２．１１、ＨｉｐｅｒＬＡＮ／２、赤外線などを始め、どのような種類の無線技術を使用することも可能であり、同様のアクセス・コントロール技術が適用可能な場合には、このリンクにおいて、例えば光ファイバなどの他の技術を使用することも可能である。また、ＷＬＡＮ管理サーバ（ＷＬＡＮサーバ）（１０２）が、ＷＬＡＮ内の別のエンティティとして存在している。このＷＬＡＮサーバ（１０２）は、アドレス空間の管理及びＷＬＡＮのリソース管理を担当しており、ＷＬＡＮのゲートウェイ上に存在するか、単純なＷＬＡＮではアクセス・ポイント（１０５）に共設されている。ＷＬＡＮサーバ（１０２）は、インターフェース（１０１５）

を介して、アクセス・ポイント（１０５）と通信を行う。これは、例えばエア・インターフェースを介するＱｏＳの管理など、ＷＬＡＮリソース・コントロールやサービス提供のためのものである。また、ＷＬＡＮを管理するため、このサーバは、例えば、不図示のＷＬＡＮゲートウェイやファイア・ウォールなど、ＷＬＡＮの他のエンティティとの相互動作を行うことも可能である。

端末のホーム・ネットワーク（１００２）では、ホーム・ネットワーク・オーソライザ（Home Network Authorizer）（１０３）がサービス許可及びアドレス割り付けの管理を行う。アクセス・ポイント（１０５）及びＷＬＡＮサーバ（１０２）は両方とも、リンク（１０１２）及びリンク（１０１４）を介して、サービス制御情報を取得するためにホーム・ネットワーク・オーソライザ（１０３）とそれぞれ通信を行う。なお、物理的に、リンク（１０１２）及びリンク（１０１４）を同一とすることも可能であり、すなわち、同一のプロトコルを使用し、同一の端末間で、同一のパケットにカプセル化された場合でも、それらは、論理上分離される。

移動端末（１０１）は、それが加入しているすべてのサービスを要求することが可能である。これらのサービスは、ホーム・ネットワーク（１００２）、個別のサービス・プロバイダ・ネットワーク（１００３）、又は、ＷＬＡＮ自体にあるかもしれない。サービスが、ホーム・ネットワーク（１００２）又はＷＬＡＮによって提供される場合には、サービス・プロバイダ・ネットワーク（１００３）は、これらのネットワークとオーバラップすることになり、コントロール機能を両方に関連付けることが可能となる。また、サービス・プロバイダ・ネットワーク管理サーバ（サービス・プロバイダ・ネットワーク・サーバ）（１０４）は、サービス許可及びサービス・プロバイダ・ネットワーク（１００３）の

アドレス割り付けを管理する。ホーム・ネットワーク・オーソライザ（１０３）は、コントロール・インターフェース（１０１３）を介して、サービス・プロバイダ・ネットワーク・サーバ（１０４）と通信を行う。実際には、サービス・プロバイダ・ネットワーク（１００３）として、ＷＬＡＮ、ホーム・ネットワーク（１００２）又は別のネットワークを利用することが可能である。また、サービスが、ホーム・ネットワーク（１００２）で提供される場合には、このインターフェースは内部インターフェースとなり、正確なフォーマットや、後述の実施例に記述されるものと同一のプロトコルを使用する必要はない。

図２は、上記のフレームワークを使用して、ＷＬＡＮ相互接続のアドレス管理のためのオペレーション･シーケンスの一例を示すものである。なお、この動作では、移動端末（ＭＴ）（１０１）がすでに、ＷＬＡＮの関連付け及び認証手続き（２０１）を終了していると仮定する。すなわち、移動端末（１０１）とアクセス・ポイント（１０５）は、相互に認証し合っており､以降のメッセージ交換のための暗号化による保護が、すでに行われている。移動端末（１０１）は、ＷＬＡＮを通じて任意のサービスにアクセスしたい場合には、リンク（１０１１）を介して、アクセス・ポイント（１０５）にMT_Request_Aメッセージ（２０２Ａ）を送信し、そのメッセージは、ホーム・ネットワーク・オーソライザ（１０３）に届けられる。このメッセージは、認証手続き（２０１）から生成されたキーによって、終端点間（エンド・トゥー・エンド）で保護されている。図３は、メッセージMT_Request_Aメッセージ（２０２Ａ）の実施例を示している。

メッセージはMessage_Typeフィールド（３０１）から始まる。このフィールドは、例えば、要求、返答など、どの種類のメッセージがカプセル化されているかを識別する。このフィールドの長さは１オクテット

であり、メッセージ・タイプは整数番号によって表わされる。これは、エア・インターフェースを通じたシグナリングに対して制限されたリソースを節約するものである。なお、必要な場合には、このフィールドが他のフォーマットも採用できることは当業者にとっては明白である。

Message_Typeフィールド（３０１）に続いて、Message_Lengthフィールド（３０２）が存在する。これは、Message_Typeフィールド（３０１）を含む全体のメッセージの長さに関する情報を含んでいる。また、次のフィールドは、Domain_Nameフィールド（３０３）である。このフィールドは、移動端末（１０１）のホーム・ドメインを識別する。なお、ネットワーク・アクセス識別子（Network Access Identifier：ＮＡＩ）（非特許文献１２）を使用することも可能であり、この場合には、例えば「UserID@home.domain.3gpp.org」の形式となる。ユーザの識別情報を保護するため、「@」記号の前のUserID部分は、例えば「roamed」などのワイルドカード値を使用する。ホーム・ドメイン情報は、移動端末（１０１）のホーム・ネットワーク・オーソライザ（１０３）に対して、メッセージをルーティングするために使用される。

上記の３つのフィールド、Message_Typeフィールド（３０１）、Message_Lengthフィールド（３０２）及びDomain_Nameフィールド（３０３）は、移動端末（１０１）とアクセス・ポイント（１０５）との間のセキュリティの関連付けによって保護される。このセキュリティの関連付けは、エア・インターフェースの保護のための認証手続き（２０１）から得られる。したがって、目的を達成するために、アクセス・ポイント（１０５）が、これらのフィールドに含まれている情報にアクセスすることが可能である。Domain_Nameフィールド（３０３）に続くフィールドは、移動端末（１０１）とホーム・ネットワーク・オーソライザ(１０３)との間のセキュリティの関連付けによって保護される。

例えば、これには、ホーム・ネットワーク・オーソライザ（１０３）のパブリック・キーが可能であり、すなわち、認証手続き（２０１）に由来したセッション・キーである、また、メッセージ保護のために使用されるキーのインデックスを示すために、Domain_Nameフィールド（３０３）のUserID部分を使用することも可能である。

Domain_Nameフィールド（３０３）の後には、MT_IDフィールド（３０４）が存在する。このフィールドは、ホーム・ネットワーク（１００２）のコンテキストにおいて、移動端末（１０１）を一意に識別するための情報を含んでいる。これは、例えば、移動端末（１０１）のＩＭＳＩ（非特許文献１３）、又は、認証手続きで獲得されたＴＭＳＩ（非特許文献１３）が可能である。ホーム・ネットワーク・オーソライザ（１０３）は、ユーザの加入情報を検索するため、この識別子を利用する。ホーム・ネットワーク・オーソライザ（１０３）が実際のユーザ識別情報にそれをマッピングすることができる限り、このフィールドに他のフォーマットを使用することも可能であることは、当業者にとっては明白である。

次のフィールドはService_Requestフィールド（３０５）である。このフィールドは、ホーム・ネットワーク・オーソライザ（１０３）に対してアクセスすることを望むサービスを示すため、移動端末（１０１）によって使用される。メッセージは、移動端末（１０１）とそのホーム・ネットワーク・オーソライザ（１０３）との間のものなので、これは、特定のオペレータ及びネットワークに特有のものである。例えば、３ＧＰＰネットワークでは、これは、使用するＧＧＳＮ及びアクセスする特別のサービスを識別するためのＡＰＮ（非特許文献１３）であり得る。ホーム・ネットワーク（１００２）が別のタイプである場合には、他のフォーマットを使用することが可能であることは、当業者にとって明白

である。さらに、例えば、帯域幅の要求など、他のサービス・リクエスト情報を追加することも可能である。フィールドに利用可能な値としては、「2M.bandwidth.request.IMS.foo.bar.operator-name.operator-group.gprs」があり得る。「request」の後の部分は、サービスを識別する標準のＡＰＮであり、また、「request」の前の部分は、特定のサービス・リクエストである。実際のリクエスト属性は、サービスに依存しており、また、オペレータが定義することも可能である。移動端末（１０１）は、ＳＩＭ又はＵＳＩＭカードから、フォーマットに関する情報を獲得することが可能である。

また、Session_IDフィールド（３０６）はセッション制御情報を提供する。これは、移動端末（１０１）が、このサービスの要求がホーム・ネットワーク・オーソライザ（１０３）に関連するセッションであることを識別するために使用される。セッションの識別子は、移動端末（１０１）内では局所的に一意であるべきであり、移動端末（１０１）は、すべてのサービス・セッションのローカルな記録を維持すべきである。新しいサービス・セッションがスタートする場合は常に、新しいセッション識別子を備えた新しいエントリが作られ、セッションが終了する場合には、そのエントリは削除されて、識別子は解放されて再利用可能となる。本実施例では、フィールドは２オクテットであり、また、識別子は１６進数の値である。なお、端末にサポートされた他のタイプの識別子の使用が可能なことは、当業者にとっては明白である。MT_IDフィールド（３０４）及びSession_IDフィールド（３０６）は、ホーム・ネットワーク・オーソライザ（１０３）において、サービス・セッションを一意に識別する。

また、Address_Requestフィールド（３０７）は、移動端末（１０１）からのアドレス割り付けの要求に関する情報を含んでいる。本実施例

では、図４に示されるように、複合した構造が使用されている。この構造の第１のパートは、Address_Typeフィールド（４０１）である。これは、どのタイプのアドレスが移動端末（１０１）にサポートされているかを識別する。このフィールドのサイズは１オクテットであり、可能な値は次の通りである。

No_IP::=0x00;

Single_Stack_IPv4::=0x01;

Single_Stack_IPv6_FullAddress::=0x02;

Single_Stack_IPv6_Prefix::=0x03;

Dual_Stack_IPv4_Preferred::=0x04;

Dual_Stack_IPv6_Preferred_FullAddress::=0x05;

Dual_Stack_IPv6_Preferred_Prefix::=0x06

さらなるタイプがサポートされ、他の数が使用され得ることは、当業者にとっては明白である。また、この構造の第２のパートは、Suggestion_Lengthフィールド（４０２）である。このフィールドは、次のフィールドAddress_Suggestionsフィールド（４０３）の長さを示している。Address_Suggestionsフィールド（４０３）は、移動端末（１０１）が割り当てられることを望むアドレスを列挙する。例えば、進行中のセッションが、あるアドレスを使用している場合、そのセッションが中断されないように同一のアドレスが割り当てられることが重要である。例えば、Address_Suggestionsフィールド（４０３）は、アドレスのリストである。リスト内の各エントリは、例えば、ＩＰｖ４やＩＰｖ６などのアドレスのタイプを示す１オクテットのタイプ・フィールドから始まり、実際のアドレスがそれに続く。端末によるアドレス提示の特徴をサポートしないホーム・ネットワーク・オーソライザ（１０３）では、Suggestion_Lengthフィールド（４０２）及び

Address_Suggestionsフィールド（４０３）は、暗黙のうちに無視される。

また、Address_Requestフィールド（３０７）の後には、Tunnel_Requestフィールド（３０８）が存在する。このフィールドは、どのタイプのトンネルをサポートしているかを示すために、移動端末（１０１）によって使用される。このフィールドの最初のオクテットは、それ自体を含むこのフィールドの長さを示し、このフィールドの内容は、２オクテットを占める各エントリを持つリストとすることが可能である。各エントリの最初のオクテットは、移動端末（１０１）がサポートするトンネル・タイプの識別子を含んでおり、そのオクテットの値には、次のものが可能である。

ネットワーク・トンネル -- 一般的::=0x01;

ネットワーク・トンネル -- モバイルIPv4::=0x02;

クライアント・トンネル -- 一般的::=0x04

クライアント・トンネル -- モバイルIPv4::=0x05;

クライアント・トンネル -- モバイルIPv6::=0x06;

トンネル無し::=0x08

このフィールドで、他のトンネルのタイプを定義して使用できることは、当業者にとっては明白である。また、各エントリの２番目のオクテットは、トンネルの方向を示している。このオクテットの可能な値は。次の通りである。

トンネル -- 端末から::=0x01;

トンネル -- 端末に::=0x02;

トンネル -- 双方向::=0x03;

リスト内の最初のエントリは、移動端末（１０１）の好ましいタイプを示している。

また、MT_Request_Aメッセージ（２０２Ａ）内の次のフィールドはWLAN_IDフィールド（３０９）である。これは、ホーム・ネットワーク・オーソライザ（１０３）に対するＷＬＡＮを識別する情報を含んでおり、これによって、ホーム・ネットワーク・オーソライザ（１０３）は、位置に基づく決定を行ったり、移動端末（１０１）への位置に基づくサービスを提供したりすることが可能となる。WLAN_IDは、認証手続きや、例えばＩＥＥＥ８０２ネットワークにおけるＳＳＩＤなどのアクセス・ポイント（１０５）からブロードキャストされた情報から取得可能である。さらに、移動端末（１０１）のローカルの識別子も含まれている。これは、アクセス・ポイント（１０５）が端末を識別するためのものである。

また、最後のフィールドは、Security_Field（３１０）である。このフィールドは、メッセージを保護するための情報を含んでいる。このフィールドのために使用される正確なアルゴリズムは、移動端末（１０１）とそのホーム・ネットワーク・オーソライザ（１０３）との間で交渉される。また、これは、ユーザの加入時間で決定されてもよく、端末のＳＩＭ又はＵＳＩＭカードに格納されてもよい。また、さらにソフトウェア・モジュールとして実施可能であり、必要な場合には常にダウンロードされるようにすることが可能である。

なお、MT_Request_Aメッセージ（２０２Ａ）内のフィールドは、上述のような正確なシーケンスに従う必要はなく、例えば、実際には、最前部にフィールドの識別子を配置する限り、任意の順にフィールド（３０４）からフィールド（３０９）を配置することが可能である。

実際には、任意の適切なメカニズムを使用して、リンク（１０１１）を通じてメッセージを伝送することが可能である。例えば、ＩＥＥＥ８０２．１１ネットワークでは、ＩＥＥＥ８０２．１ｘに定義されるＥＡ

ＰＯＬを使用し、ＥＡＰメッセージとして実現することが可能である（非特許文献１４）。

アクセス・ポイント（１０５）がこのメッセージを受け取った場合には、Domain_Nameフィールド（３０３）からホーム・ドメイン情報を引き出し、例えば、ＤＮＳの照会を行なうなど、そのドメイン情報を利用して、ホーム・ネットワーク・オーソライザ（１０３）のアドレスを取得することが可能である。アクセス・ポイント（１０５）は、この情報に従って、対応するホーム・ネットワーク・オーソライザ（１０３）にメッセージを転送する。例えば、ＷＬＡＮがセントラルＡＡＡサーバを有する場合には、アクセス・ポイント（１０５）は、ＡＡＡサーバにメッセージを直接転送する。そして、ＷＬＡＮのＡＡＡサーバはドメイン情報を解析し、実際のホーム・ネットワーク・オーソライザ（１０３）にメッセージを転送する。なお、アクセス・ポイント（１０５）とホーム・ネットワーク・オーソライザ（１０３）との間に、安全なリンクが存在することを前提としており、これは、認証手続き（２０１）での設定で可能となるか、又は、そのプロセスに由来するセキュリティの関連付けを動的に設定することによって可能となる。

また、アクセス・ポイント（１０５）は、メッセージ処理に参加する必要がなく、したがって、メッセージを解析するためにスタック全体を実施する必要がない。それは、単にメッセージ・タイプを読み、MT_Request_Bメッセージ（２０２Ｂ）のステップとして示される再カプセル化及び転送を行う必要があるだけである。転送のために使用されるプロトコルとしては、任意の適切なＡＡＡプロトコル（例えば、ダイアメータのためのＥＡＰアプリケーション（非特許文献１５）や、ダイアメータのためのＮＡＳＲＥＱアプリケーション（非特許文献１６））が可能である。それらのプロトコルは、認証を目的として、アクセス・

ポイント（１０５）において、すでに利用可能である。したがって、メッセージMT_Request_Aメッセージ（２０２Ａ）は、終端点間の認証手続き（２０１）と同様、本質的には、移動端末（１０１）からホーム・ネットワーク・オーソライザ（１０３）にエンド・トゥー・エンドで送られる。

また、図５は、ホーム・ネットワーク・オーソライザ（１０３）の状態マシンの実施例を示すものである。ホーム・ネットワーク・オーソライザ（１０３）は、初期状態（５０１）から始まり、遷移（/intiate()）（５００１）で初期化（）の処理を行ってアイドル状態（５０２）に移る。初期化（）プロセスは、他のバックエンド・サーバとの接続、セキュリティの関連付けなどを確立するために必要なすべてのステップを含んでいる。実際には、設定に依存して他のプロセスが含まれ得ることは、当業者にとっては明白である。

ホーム・ネットワーク・オーソライザ（１０３）が、遷移（５００２）でアクセス・ポイント（１０５）から転送されたMT_Request_Bメッセージ（２０２Ｂ）を受け取った場合には、メッセージ復号状態（５０３）に遷移する。図６は、メッセージ復号状態（５０３）の実施例を示すものである。メッセージ復号状態（５０３）では、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６００１）でDomain_Nameフィールド（３０３）によって識別されたキーを使用して、MT_Request_Bメッセージ（202B）内のフィールドを復号する。ステップ（６００２）において、メッセージが破損されているか、又は、Security_Field（３１０）を使用して修正されていることを検知した場合、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６０１３）において、不正なメッセージのフラグをセットし、状態マシンは、遷移（５００４）でサービス却下状態（５０４）に遷移する。

MT_Request_Bメッセージ（２０２Ｂ）から、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６００３）において、MT_IDフィールド（３０４）から端末の識別情報に関する情報を獲得することが可能である。この識別情報を使用して、ホーム・ネットワーク・オーソライザ（１０３）は、そのデータベースやバックエンド・サーバ（例えば、３ＧＰＰネットワークのＨＳＳ）から、ユーザの加入情報を検索する。また、ホーム・ネットワーク・オーソライザ（１０３）は、さらにステップ（６００４）で、Service_Requestフィールド（３０５）から得られたサービス要求情報を解析する。サービス要求は、例えば、帯域幅、遅れ、不安定性など、挿入される様々なサービス固有情報を含むことが可能である。ステップ（６００５）において、ホーム・ネットワーク・オーソライザ（１０３）内では、ユーザ加入情報を使用して、ユーザにサービスを与えないでおくべきかどうかに関する決定が下される。ユーザの加入に基づいて、要求されたサービスが与えられるべきではないとされた場合、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６０１３）において、サービスを否定するフラグをセットし、状態マシンは、遷移（５００４）でサービス却下状態（５０４）に遷移する。もしサービスが許される場合には、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６００７）において、Session_IDフィールド（３０６）において受信したセッション識別子のサービスの端末を求めて、そのレコードを探索する。同一セッション識別子を有するレコードが存在する場合には、これがハンドオーバの要求であることを意味し、端末には同じアドレスが割り当てられるべきである。これにより、サービス・セッションは中断されることがなくなる。また、レコードが存在しない場合には、それは新しい要求であることを意味し、ステップ（６００８）において、レコード・エントリが生成され、ホーム・

ネットワーク・オーソライザ（１０３）の格納部に格納されるか、例えば、ＨＳＳなどのバックエンド・データベースが更新される。ホーム・ネットワーク・オーソライザ（１０３）は、さらにサービス情報を使用して、サービス・プロバイダ・ネットワーク（１００３）を識別し、サービス・プロバイダ・ネットワーク・サーバ（１０４）との接続がセット・アップされる。

ステップ（６００９）において、Address_Requestフィールド（３０７）から、ホーム・ネットワーク・オーソライザ（１０３）は、移動端末（１０１）が使用を望んでいるアドレスを取得する。なお、ホーム・ネットワーク・オーソライザ（１０３）が、オペレータのポリシーやその他によって、この機能をサポートしたくない場合、この情報を暗黙に無視することが可能である。移動端末（１０１）は、ホーム・ネットワーク・オーソライザ（１０３）から割り当てられた最終的なアドレスを常に使用するべきである。ホーム・ネットワーク・オーソライザ（１０３）は、要求されたサービスから、アドレスが、局所的に又はホーム・ネットワーク（１００２）内で割り当てられるべきか、あるいは、サービス・プロバイダ・ネットワーク（１００３）内で割り当てられるべきかを決定する。例えば、ユーザがＷＬＡＮローカル・サービスを利用することしか認められていなければ、アドレスはＷＬＡＮ内で割り当てられ、一方、ＶＰＮサービスに加入するユーザには、そのＶＰＮ内のアドレスを用いて割り当てられるべきである。

また、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６０１０）でTunnel_Requestフィールド（３０８）から、移動端末（１０１）にサポートされたトンネルのタイプを検索する。この情報は、サービス提供のためにトンネルをセット・アップするために用いられる。移動端末（１０１）は、１つ以上のトンネルのタイプを列挙し、リスト

中の最初のものを好ましいタイプのものとすることが可能である。ホーム・ネットワーク・オーソライザ（１０３）は、サービス・プロバイダ・ネットワーク・サーバ（１０４）と共にチェックを行って、どのタイプを使用すべきであるか決定する必要がある。なお、例えば、トンネルの方向などの付加的な情報が含まれてもよい。

ステップ（６０１１）において、ホーム・ネットワーク・オーソライザ（１０３）は、WLAN_IDフィールド（３０９）から、移動端末（１０１）が現在関係している無線ＬＡＮの識別情報を得る。この情報を使用して、ホーム・ネットワーク・オーソライザ（１０３）は、対応するＷＬＡＮ管理サーバ（１０２）を見つける。なお、ローミングの協定の一部として、ホーム・ネットワーク・オーソライザ（１０３）のデータベースにこの情報を格納することが可能であり、また、バックエンド・サーバ（例えばＨＳＳ）からこの情報を引き出せるようにすることも可能である。サーバの情報を取得した後、安全なリンクが確立される。このリンクは、以降のサービス・メッセージ・シグナリングのために使用されるものである。

すべての情報を取得した後、ホーム・ネットワーク・オーソライザ（１０３）は、Service_Reqeustメッセージ（２０３）及びWLAN_Requestメッセージ（２０５）を作成し、ホーム・ネットワーク・オーソライザ（１０３）の状態マシンが待機状態（５０４）に遷移する場合、このメッセージが送り出される。

図７は、Service_Requestメッセージ（２０３）の実施例を示すものである。このメッセージは、Home_Network_IDフィールド（７０１）から始まる。このフィールドは、移動端末（１０１）のホーム・ネットワーク識別子に関する情報を含み、オペレータの名前や大きなネットワークのサブシステムであり得る。識別子はグローバルにユニークでなけ

ればならず、例えば「network.operator.3gpp.org」などのネットワークのＤＮＳ名は、この識別子の好適な候補である。ホーム・ネットワーク情報の存在によって、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、例えば、ローミングの協定などのネットワーク・ポリシーを、サービス要求に対して適用することが可能となる。また、ユーザのプロファイルはホーム・ネットワーク（１００２）によって管理されている。したがって、ユーザ情報は、サービス・プロバイダ・ネットワーク・サーバ（１０４）に送られるべきではないが、サービスのよりよいコントロールを可能にするため、メッセージにユーザ・プライオリティ／グルーピング情報を付加することも可能である。これは、例えば、「goldmember.network.operator.3gpp.org」などのように、ホーム・ネットワーク識別子と関連付けられてもよい。サービス・プロバイダ・ネットワーク・サーバ（１０４）は、これを用いて、サービスを与える場合にユーザを差別化することが可能となる。

また、次のフィールドはMT_IDフィールド（７０２）である。このフィールドは、移動端末（１０１）の識別子に関する情報を含んでおり、ホーム・ネットワーク・オーソライザ（１０３）がサービス・トラッキングを行うために使用される。識別子は端末のＩＭＳＩ、又は、ホーム・ネットワーク・オーソライザ（１０３）によって割り当てられ、サービス・セッションに固有の一時的なＩＤであり得る。なお、この情報は、サービス・セッションが終了するまで一貫性を有している必要がある。

また、上記のフィールドに続いて、Session_IDフィールド（７０３）が存在する。これは、端末によって割り当てられたセッション識別子である。サービス・プロバイダ・ネットワーク・サーバ（１０４）は、現在行われているすべてのセッション情報の記録を保持すべきである。したがって、セッション識別子がデータベースに存在する場合には、それ

は、サービス要求がハンドオーバによって引き起こされることを意味し、また、サービスの中断を避けるために同一のアドレス構成を使用すべきであることを意味する。例えば、セッションが稼動している（アクティブ）場合、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、移動端末（１０１）に対して同一のアドレスを割り当てるべきである。その結果、コレスポンデント・ノードとの通信はシグナリングなしで継続されるようにすることが可能となる。

また、Address_Requestフィールド（７０４）は、MT_Request_Aメッセージ（２０２Ａ）のものと同一である。この部分は、例えば、ＩＰｖ６などの割り当てるべきアドレスのタイプをサービス・プロバイダ・ネットワーク・サーバ（１０４）に示すものである。さらに、MT_Request_Aメッセージ（２０２Ａ）のAddress_Requestフィールド（３０７）と同様に、移動端末（１０１）によって要求されたアドレスを提供する。なお、サービス・プロバイダ・ネットワーク・サーバ（１０４）がこの機能をサポートしたくない場合には、この情報を無視すればよい。また、ホーム・ネットワーク・オーソライザ（１０３）によってサービス・プロバイダ・ネットワーク（１００３）からアドレスを割り当てられる必要がないと決定された場合には、このフィールドは省略されてもよい。

Service_Specフィールド（７０５）は、複合したフィールドであり、ユーザの加入情報に基づいてホーム・ネットワーク・オーソライザ（１０３）から要求される特定の要件に関する情報を含んでいる。このフィールドの可能な実施例（データ構造１）は、以下に示される。

```
struct Service_Spec{
        u_long   bitrate_avg;
        u_long   bitrate_max;
```

```
int   deliver_order;
int   MTU_size;
double   delay;
double   jitter;
int   priority;
int   service_direction;
int   QoS_type
struct   timeval   start_time;
struct   timeval   end_time;
};
```

この属性のうち、bitrate_avg及びbitrate_maxは、要求されたサービスを保証するビット・レート及び最大のビット・レートである。また、deliver_orderの属性は、配送が順番に行われるかどうかを示すものである。また、MTU_sizeは、サービスのために転送される最大のデータ・ユニット・サイズを特定するものである。また、delayとjitterのフィールドは、サービスのためのいくつかの基本的なＱｏＳの属性を指定するものである。また、priorityの属性は、このサービスのためのデータ・トラフィックの取り扱い優先度を示すものである。また、service_directionの属性は、サービスが一方向か双方向かを示すものである。また、QoS_typeの属性は、例えばDiffServ、あるいはＲＳＶＰなどを備えたInterServサービスなどのサービスを提供するために用いられるＱｏＳのスキームを示すものである。また、start_time及びend_timeは、サービスの開始時間及び終了時間を示すものである。サービス・プロバイダ・ネットワーク・サーバ（１０４）は、この情報を用いて、サービスのためのリソースのスケジュールを決めることが可能である。なお、実際に実施される際の構造においては、サービスに固有の

他の属性が含まれてもよいことは、当業者にとっては明白である。

また、Service_Specフィールド（７０５）の後には、Tunnel_Specフィールド（７０６）が存在する。このフィールドはトンネル情報を含んでおり、MT_Request_Aメッセージ（２０２Ａ）のTunnel_Requestフィールド（３０８）と同様だが、いくつかの特別な情報が付加されている。例えば、ネットワーク・トンネル・エントリに関しては、ＷＬＡＮの終端点が提供され、端末のトンネルに関しては、データ暗号化のために、セキュリティ・キーを付加することが可能である。

また、Service_Requestメッセージ（２０３）の最後のフィールドは、Security_Field（７０７）である。このフィールドは、ホーム・ネットワーク・オーソライザ（１０３）とサービス・プロバイダ・ネットワーク・サーバ（１０４）との間のセキュリティの関連付けを用いて、メッセージ全体を保護するために使用される。なお、ここで使用される正確なアルゴリズムは、実際の実施形態に依存する。

なお、Service_Requestメッセージ（２０３）内のフィールドが記述された順序である必要がないことは、当業者にとっては明白であり、実際には、ホーム・ネットワーク・オーソライザ（１０３）及びサービス・プロバイダ・ネットワーク・サーバ（１０４）は、シグナリングの最適化のために、任意の適切な順序の交渉を行うことも可能である。

サービス・プロバイダ・ネットワーク・サーバ（１０４）は、Service_Requestメッセージ（２０３）を受け取った後、サービス・アドレス管理（２０４）手続きを行なう。この手続きでは、サービス・プロバイダ・ネットワーク・サーバ（１０４）が、Session_ID（７０３）に含まれていたセッション識別子を求めて、そのデータベースの探索を行う。同一の移動端末（１０１）のセッション識別子が存在する場合、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、例えば、

ＭＴのアドレス、サービスの詳細など、その記録内のすべての情報をコピーし、それを返答メッセージとしてホーム・ネットワーク・オーソライザ（１０３）に直接返信する。

また、セッション識別子が存在しない場合には、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、そのデータベースの指標（インデックス）として、新しいセッション識別子を使用して新しいエントリを作成する。サービス・プロバイダ・ネットワーク・サーバ（１０４）は、Address_Requestフィールド（７０４）をチェックし、このフィールドで指定されたアドレスのタイプに基づいて、移動端末（１０１）に適切なアドレスを割り当てる。

サービス・プロバイダ・ネットワーク・サーバ（１０４）は、ホーム・ネットワーク・オーソライザ（１０３）からのService_Specフィールド（７０５）をチェックし、要求されたサービスがサポートされない場合には、失敗を示すメッセージが、ホーム・ネットワーク・オーソライザ（１０３）に送られる。なお、失敗の原因を特定するために、あるエラー・コードを使用することも可能である。また、Service_Specフィールド（７０５）内の所定の属性が、サービス・プロバイダ・ネットワーク（１００３）の現在の能力を超える場合には、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、新しいセットの属性で、ホーム・ネットワーク・オーソライザ（１０３）とやり取りを行おうと試みることも可能である。これは、サービス・プロバイダ・ネットワーク・サーバ（１０４）によって提案された値に修正されたService_Specフィールド（７０５）を有する同一のService_Requestメッセージ（２０３）が、ホーム・ネットワーク・オーソライザ（１０３）に送り返されることによって達成される。

また、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、

Tunnel_Sepcフィールド（７０６）をチェックし、一致するトンネルのタイプを求める。複数の一致があるかもしれないが、サービス・プロバイダ・ネットワーク・サーバ（１０４）は最初に一致したものを選択すべきである。ネットワークに基づくトンネルのタイプに関しては、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、返答メッセージ内にトンネルの終端点の情報を用意する必要がある。クライアントに基づくトンネルに関しては、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、トンネルのタイプに固有の情報を用意し、返答情報にこの情報を含ませる。例えば、モバイルＩＰｖ６のタイプのスキームに関しては、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、移動端末（１０１）にホーム・エージェントを割り当てる必要がある。また、返答メッセージ内に、あるセキュリティ情報を含ませることも可能である。なお、方向性の情報（例えば、一方向、両方向）もトンネル情報のフィールドに付加されてもよい。

サービス・プロバイダ・ネットワーク・サーバ（１０４）は、Service_Replyメッセージ（２０５）を用いて、ホーム・ネットワーク・オーソライザ（１０３）に対して返答を行う。Service_Replyメッセージ（２０５）には、図７に示されるようなService_Requestメッセージ（２０３）と同様の構造を使用することが可能である。

Home_Network_IDフィールド（７０１）、MT_IDフィールド（７０２）、及び、Session_IDフィールド（７０３）の内容は、対応するService_Requestメッセージ（２０３）から直接コピーされる。なお、これらのフィールドは、複数の端末のためにシグナリングのリンクが再利用される場合に、要求及び返答メッセージのペアを一致させるために、ホームネットワークオーソライザ（１０３）によって使用される。

Service_Replyメッセージ（２０５）内のAddress_Requestフィールド

（７０４）の内容は、移動端末（１０１）に割り当てられたアドレスを含んでおり、それは、バイトでフィールドの長さを示す最初のオクテットを有するアドレスのエントリのリストであり得る。フィールドの次の部分はアドレスのリストであり、実際のアドレスを伴うアドレスのタイプを示す１オクテットを有している。ワイルドカードのアドレスも許可されており、例えば、アドレス・フィールドがすべて０で満たされる場合には、ＷＬＡＮのローカルのメカニズム（例えばＩＰｖ６自動割り付け（非特許文献１７）やＤＨＣＰを使用して、移動端末（１０１）がアドレスを形成することを示している。

また、Service_Replyメッセージ（２０５）内のService_Specフィールド（７０５）の内容には、サービス・プロバイダ・ネットワーク・サーバ（１０４）によって同意された属性が含まれている。すべての属性がサービス・プロバイダ・ネットワーク・サーバ（１０４）によって承認される場合には、対応するService_Requestメッセージ（２０３）内のService_Specフィールド（７０５）と同一である。一方、同一でない場合には、サービス・プロバイダ・ネットワーク・サーバ（１０４）は、ホーム・ネットワーク・オーソライザ（１０３）に対して、対立した提案を行っていることになる。

また、Service_Replyメッセージ（２０５）内のTunnel_Specフィールド（７０６）は、サービス・プロバイダ・ネットワーク・サーバ（１０４）によって選択されたトンネルの設定を含んでいる。このフィールドの正確な内容は、トンネルのタイプに依存しており、クライアントに基づくトンネル・タイプが選択された場合には、ただ１つのセッティングのみが必要となる。例えば、もしモバイルＩＰｖ６が同意されていれば、このフィールドには、移動端末（１０１）に割り当てられたホーム・エージェントのアドレス及びバインディングアップデート認証のためのセ

キュリティ・キーなどが含まれることとなる。また、Address_Requestフィールド（７０４）内のアドレスは、移動端末（１０１）のホーム・アドレスとして使用される。また、ネットワークに基づくトンネルのタイプが選択される場合、このフィールドには、例えば、終端点アドレスやトンネル識別子、サポートされるトンネルのタイプのそれぞれに関して必要となるすべての詳細な情報が含まれることとなる。

Service_Requestメッセージ（２０３）と並行して、ホーム・ネットワーク・オーソライザ（１０３）は、ＷＬＡＮサーバ（１０２）に対して、WLAN_Requestメッセージ（２０６）を送信する。このメッセージは、ＷＬＡＮ内のサービス提供に必要な設定の取り決めを行うためのものである。図８には、このメッセージの実施例が示される。

WLAN_Requestメッセージ（２０６）は、Service_Requestメッセージ（２０３）のように、Home_Network_IDフィールド（８０１）及びMT_IDフィールド（８０２）の２つのフィールドを含んでいる。

Home_Network_IDフィールド（８０１）は、加入者のホーム・ネットワークの識別子を含んでおり、あるネットワーク・ポリシーがサービス提供に適用される場合に、ＷＬＡＮサーバ（１０２）に渡される。また、MT_IDフィールド（８０２）は、移動端末（１０１）の位置を追跡するために使用される。例えば、移動端末（１０１）の下位レイヤの識別子（例えば、ＭＡＣアドレス）と関連するアクセス・ポイントの識別子を利用することが可能である。

また、Address_Allocフィールド（８０３）は、移動端末（１０１）にＷＬＡＮのローカル・アドレスを割り当てる必要があるかどうか示すフラグと、使用されるべきアドレスのタイプである。ホーム・ネットワーク・オーソライザ（１０３）は、選択されたトンネル・スキームに基づいて、ローカル・アドレスが必要か否かを決定する。実際には、例え

ば、次の定義を用いて、このフィールドの最初のオクテットによって、アドレス割り付けが必要であるか否かが示される。

No_Allocation::=0x00;

Single_Stack_IPv4::=0x01;

Single_Stack_IPv6_FullAddress::=0x02;

Single_Stack_IPv6_Prefix::=0x03;

Dual_Stack_IPv4_Preferred::=0x04;

Dual_Stack_IPv6_Preferred_FullAddress::=0x05;

Dual_Stack_IPv6_Preferred_Prefix::=0x06

なお、このメッセージの実際の実施において、他の値が使用可能であることは、当業者にとっては明白である。

Service_Supportフィールド（８０４）は、ＷＬＡＮ内でサービス提供をサポートするために必要な属性をすべて含んでいる、複合したフィールドである。実際の内容は、サービスの特定であり、このフィールドの内容の例は、データ構造１に説明されたものである。

また、Tunnel_Setupフィールド（８０５）も複合したフィールドであり、Service_Requestメッセージ（２０３）内のTunnel_Specフィールド（７０６）と同様のフォーマットが使用される。

また、WLAN_Requestメッセージ（２０６）の最後のフィールドは、Security_Field（８０６）である。このフィールドは、メッセージ全体を完全に保護するために、セキュリティの関連付けが使用される。このフィールドの計算のために使用されるアルゴリズムは、実際の実施形態に依存している。

WLAN_Requestメッセージ（２０６）を受け取った後、ＷＬＡＮサーバ（１０２）は、ＷＬＡＮサービス・アドレス管理（２０７）を実行する。例えば、ローカルのＩＰｖ６アドレスの割り付けが、ホーム・ネッ

トワーク・オーソライザ（１０３）によって要求された場合には、ＷＬＡＮサーバ（１０２）は、適切なネットワーク・セクションを見つけて、端末にＩＰｖ６アドレスを割り当てる。なお、必要ならば、さらにＷＬＡＮサーバ（１０２）は、ゲートウェイの更新を行う（すなわち、ＷＬＡＮのファイア・ウォールに新しいアドレスの割り付けを行う）。これにより、移動端末（１０１）は、この割り当てられたローカル・アドレスを使用して、サービスにアクセスすることが可能となる。

ＷＬＡＮサーバ（１０２）は、さらにローカルの承認コントロールを実行するために、Service_Supportフィールド（８０４）内の情報を使用する。サービス・プロバイダ・ネットワーク・サーバ（１０４）と同様に、もし任意の属性がＷＬＡＮの現在のキャパシティーを超える場合には、ＷＬＡＮサーバ（１０２）は、ホーム・ネットワーク・オーソライザ（１０３）との間で、例えば、ビット・レートの縮小やサービスの時間間隔の変更など、サービスの詳細に係る新しいセットの取り決めを試みる。

もし、クライアントに基づくトンネルのスキームが、ホーム・ネットワーク・オーソライザ（１０３）によって選択された場合には、ＷＬＡＮサーバ（１０２）は、特別な設定を行う必要がない。一方、ネットワークに基づくトンネル・スキームが使用される場合には、ＷＬＡＮサーバ（１０２）は、MT_IDフィールド（８０２）からの情報を用いて、トンネルの終端点を識別する必要がある。

ＷＬＡＮサーバ（１０２）は、WLAN_Replyメッセージ（２０８）を用いて、WLAN_Requestメッセージ（２０６）への返答を行う。WLAN_Replyメッセージ（２０８）には、図８に示されるWLAN_Requestメッセージ（２０６）と同様の構造が利用される。Home_Network_IDフィールド（８０１）とMT_IDフィールド（８０２

）は、対応するWLAN_Requestメッセージ（２０６）から直接コピーされる。これらのフィールドは、要求及び返答メッセージのペアを一致させるために、ホーム・ネットワーク・オーソライザ（１０３）によって使用される。

また、WLAN_Replyメッセージ（２０８）内のAddress_Allocフィールド（８０３）には、移動端末（１０１）に割り当てられたＷＬＡＮのローカル・アドレスの情報が含まれている。MT_Request_Aメッセージ（２０２Ａ）内のAddress_Requestフィールド（３０７）に定義されるように、このフィールドの最初のオクテットは、アドレスのタイプを示している。このフィールドの次に続く部分には、移動端末（１０１）に割り当てられる実際のアドレスが含まれており、例えば、ＩＰｖ６アドレスが割り当てられる場合には、最初のオクテットは0x02となり、次の３２オクテットには、実際のＩＰｖ６アドレスが含まれる。

また、WLAN_Replyメッセージ（２０８）内のService_Supportフィールド（８０４）には、WLAN_Requestメッセージ（２０６）に定義されるサービスの属性の情報が含まれている。もし、ＷＬＡＮがこれらのサービスの属性を受け入れた場合には、ＷＬＡＮサーバ（１０２）は、WLAN_Requestメッセージ（２０６）から、それらを直接コピーする。一方、ＷＬＡＮサーバ（１０２）がその属性を受け入れることができなかった場合、WLAN_Replyメッセージ（２０８）内に新しい値をセットした属性を加えて、新たな提案を送信する。

また、WLAN_Replyメッセージ（２０８）内のTunnel_Setupフィールド（８０５）は、移動端末（１０１）へのトンネルの情報である。ここには、最初のオクテット内で使用されるトンネルのタイプ、及び、次のオクテットでトンネルのタイプに固有のデータが示されている。例えば、モバイルＩＰｖ６がデータ・トラフィックに対して使用される場合

には、このフィールド内にはトンネルのタイプのみが存在し、Address_Allocフィールド（８０３）のアドレスが移動端末（１０１）の気付アドレスとして使用される。一方、モバイルＩＰｖ４が使用される場合には、このフィールドには、最初のオクテットにトンネルのタイプが含まれ、移動端末（１０１）に割り当てられるフォーリン・エージェントのアドレスが後続する。

Service_Replyメッセージ（２０５）及びWLAN_Replyメッセージ（２０８）の受信後、ホーム・ネットワーク・オーソライザ（１０３）は、ＷＬＡＮサーバ（１０２）及びサービス・プロバイダ・ネットワーク・サーバ（１０４）からの情報を統合する。もし、Service_Specフィールド（７０５）又はService_Supportフィールド（７０６）が、Service_Requestメッセージ（２０３）又はWLAN_Requestメッセージ（２０６）内のものとは異なっている属性の値を含んでいる場合には、サービスの詳細を再度取り決める必要がある。このとき、ホーム・ネットワーク・オーソライザ（１０３）は、サービス・プロバイダ・ネットワーク・サーバ（１０４）又はＷＬＡＮサーバ（１０２）によって提案された新しい値をチェックし、もし、これらの新しい値を受け入れることが可能ならば、SPN_Configメッセージ（２１０）及びWLAN_Configメッセージ（２１１）を用いて、新しい設定の承認を行う。

Service_Requestメッセージ（２０３）、Service_Replyメッセージ（２０５）とWLAN_Requestメッセージ（２０６）、WLAN_Reply messagge（２０８）とのメッセージのペアは、時間的な相関性を有していない。すなわち、それらは並行に行われるか、ホーム・ネットワーク・オーソライザ（１０３）の実施にそれぞれ依存して１つずつ行われる。例えば、ＷＬＡＮサーバ（１０２）との接続がアイドル状態ならば、ホーム・ネットワーク・オーソライザ（１０３）は、Service_Requestメ

ッセージ（２０３）の代わりにWLAN_Requestメッセージ（２０６）を発送する決定を行うことが可能である。

また、再度やり取りが必要な場合に、新しいサービス・パラメータを確認するために、ホーム・ネットワーク・オーソライザ（１０３）からサービス・プロバイダ・ネットワーク・サーバ（１０４）に対して、SPN_Configメッセージ（２１０）が送られる。なお、SPN_Configメッセージ（２１０）には、Service_Requestメッセージ（２０３）と同一のメッセージ・フォーマットが使用される。また、もし同一のメッセージ・フォーマットを使用しない場合には、例えば、Address_Requestなどのいくつかのフィールドが省略されることがある。

また、必要に応じて、トンネリングの情報が付加されてもよい。例えば、クライアントに基づくトンネル（例えば、モバイルＩＰ）が使用される場合には、ＷＬＡＮサーバ（１０２）によって割り当てられる移動端末（１０１）の気付アドレスが、Tunnel_Requestフィールド（３０８）に挿入される。また、ネットワークに基づくトンネルが使用される場合には、ＷＬＡＮのトンネルの終端点アドレスやポート番号などが、このメッセージで転送される。

また、WLAN_Configメッセージ（２１１）は、同様の目的で利用されるものであり、ホーム・ネットワーク・オーソライザ（１０３）は、必要に応じて、このメッセージを使用して、ＷＬＡＮサーバ（１０２）に新しい設定を確認してもらう。また、さらに、この情報は、トンネルの情報を転送するために用いられることも可能である。例えば、ネットワークに基づくトンネルが使用される場合には、サービス・プロバイダ・ネットワーク（１００３）のトンネルの終端点アドレスやポート番号などが、このメッセージでＷＬＡＮサーバ（１０２）に転送され、その後、ＷＬＡＮサーバ（１０２）は、コレスポンデント・ノードに対して、

トンネルをセット・アップするよう命ずる。一方、クライアントに基づくトンネルが使用される場合には、端末のアドレスがこのメッセージに含まれ、その結果、ＷＬＡＮはデータ・トラフィックのためにファイア・ウォールを開くことが可能となる。

なお、サービス・セッションが終わったときに、移動端末（１０１）に割り当てられたリソースを無効にするために、ホーム・ネットワーク・オーソライザ（１０３）によって、これらの２つのメッセージ、SPN_Configメッセージ（２１０）及びWLAN_Configメッセージ（２１１）が使用可能であることは、当業者にとっては明白である。例えば、移動端末（１０１）がもはやＷＬＡＮ内に存在しないことを、ホーム・ネットワーク・オーソライザ（１０３）が検知した場合には、それは、すべて０にセットされたService_Supportフィールド（８０４）を含むWLAN_Configメッセージ（２１１）を出すことができる。ＷＬＡＮサーバ（１０２）は、この種のメッセージを受け取った後、移動端末（１０１）に割り当てられたリソースをすべて解放し、他の適切な動作を実行する。

ホーム・ネットワーク・オーソライザ（１０３）は、MT_Request_Bメッセージ（２０２Ｂ）に対する返答として、MT_Reply_Bメッセージ（２１２Ｂ）を送る。このメッセージは、アクセス・ポイント（１０５）、又は、他の付随した装置によって、メッセージMT_Reply_Aメッセージ（２１２Ａ）として、移動端末（１０１）に転送される。なお、MT_Reply_Aメッセージ（２１２Ａ）及びMT_Reply_Bメッセージ（２１２Ｂ）は、同一の内容及びフォーマットを有している。ホーム・ネットワーク・オーソライザ（１０３）と移動端末（１０１）との間のネットワーク・エレメントは、これらのメッセージの内容にアクセスせず、また、アクセス・ポイント（１０５）は、単にメッセージ全体を再カプ

セル化して、それを転送する。MT_Reply_Aメッセージ（２１２Ａ）又はMT_Reply Bメッセージ（２１２Ｂ）は、移動端末（１０１）とホーム・ネットワーク・オーソライザ（１０３）との間で共有されるセキュリティの関連付けによって暗号化される。なお、MT_Reply_Aメッセージ（２１２Ａ）は、対応するMT_Request_Aメッセージ（２０２Ａ）への返答であり、アクセス・ポイント（１０５）は、転送すべき移動端末（１０１）を把握することが可能である。

また、ＷＬＡＮサーバ（１０２）がMT_Reply_B_message（２１２Ｂ）のパス上にある場合には、そのメッセージにWLAN_Configメッセージ（２１１）を乗せて運ぶことが可能である。例えば、ＷＬＡＮサーバ（１０２）が、ＷＬＡＮ内のダイアメータを用いて、移動端末（１０１）にMT_Reply_Bメッセージ（２１２Ｂ）を転送するＡＡＡサーバである場合には、MT_Reply_Bメッセージ（２１２Ｂ）は、ダイアメーターＥＡＰ－Answer ＡＶＰにカプセル化可能である。一方、同じメッセージ内の別のＡＶＰにWLAN_Configメッセージ（２１１）がカプセル化されてもよい。また、他の転送プロトコルが利用される場合でも、同じようなスキームが使用可能であることは、当業者にとっては明白である。

また、MT_Reply_Aメッセージ（２１２Ａ）は、図３に示されるMT_Request_Aメッセージ（２０２Ａ）と同一の構造を有している。Message_Typeフィールド（３０１）は、MT_Request_Aメッセージ（２０２Ａ）のものと同一のフォーマットを有しており、このメッセージが要求ではなく、返答であることを示すための整数が使用される。また、Message_Lengthフィールド（３０２）は、Message_Typeフィールド（３０１）を含むメッセージの長さの合計を示すものである。また、MT_Reply_Aメッセージ（２１２Ａ）内のDomain_Nameフィールド（３０３）及びMT_IDフィールド（３０４）は、MT_Request_Aメッセー

ジ（２０２Ａ）内のものと同一である。なお、シグナリングを最適化するため、実際には、これらのフィールドが省略可能であることは、当業者にとっては明白である。

また、MT_Reply_Aメッセージ（２１２Ａ）内のService_Requestフィールド（３０５）は、ユーザの加入情報に基づいて、ホーム・ネットワーク・オーソライザ（１０３）によってセットされるサービス特定情報を含むように使用される。例えば、もしユーザがＩＭＳサービスを要求した場合には、Ｐ－ＣＳＣＦアドレスが利用可能である。なお、このフィールドが、サービスの提供に必要な他の情報を含んでもよいことは、当業者にとっては明白である。また、このフィールドの正確なフォーマットは、サービスに依存している。

また、MT_Reply_Aメッセージ（２１２Ａ）内のSession_IDフィールド（３０６）は、MT_Request_Aメッセージ（２０２Ａ）から直接コピーされるが、移動端末（１０１）によって要求されない場合、実際にはそれを省略することが可能である。

また、MT_Reply_Aメッセージ（２１２Ａ）内のAddress_Requestフィールド（３０７）は、移動端末（１０１）に割り当てられるアドレスを含んでいる。これは、ソース・アドレスとしてサービス・アプリケーションによって使用されるべきものである。このフィールドの最初のオクテットはアドレスのタイプであり、実際のアドレスが後続する。例えば、もしＩＰｖ６アドレスのプリフィックスが割り当てられれば、最初のオクテットは0x03となる。また、次の３２オクテットは、実際のIPv6アドレスを形成するために移動端末（１０１）によって使用されるプリフィックス情報を含んでおり、例えば、ＷＬＡＮゲートウェイアドレス、ＤＮＳサーバアドレスなどの他のアドレス情報を含むことも可能である。これらの属性は、上記のアドレス情報に後続する。また、すべて０であ

るワイルドカードの値は、移動端末（１０１）が、実際のアドレス情報を得るために、ローカルのステートレス（Stateless）のメカニズムを使用すべきであることを示している。

また、MT_Reply_Aメッセージ（２１２Ａ）内のTunnel_Requestフィールド（３０８）は、移動端末（１０１）によって要求されるサービスにアクセスするためのトンネリングの設定を含むものである。これは、トンネルのタイプに依存し、このフィールドの最初のオクテットは、使用されるトンネルのタイプを示している。

例えば、クライアントに基づくトンネルのタイプにモバイルＩＰｖ６が使用される場合には、MT_Request_Aメッセージ（２０２Ａ）でトンネルのタイプが定義されるように、その値は0x06となる。タイプの属性に続いて、ＷＬＡＮによって割り当てられる気付アドレス及びホーム・エージェントのアドレス、そして、必要であればセキュリティ・キーが存在する。Address_Requestフィールド（３０７）内のアドレスは、端末に割り当てられたホーム・アドレスとなる。

また、ネットワークに基づくトンネルのタイプが使用された場合には、タイプ属性に続いて、トンネルのローカルの終端点アドレスと、移動端末（１０１）が安全に終端点と通信を行うためのセキュリティ・キーとが存在する。

MT_Reply_Aメッセージ（２１２Ａ）内のWLAN_IDフィールド（３０９）は、MT_Request_Aメッセージ（２０２Ａ）から直接コピーされる。なお、シグナリングを最適化するため、実際には、それを省略することが可能である。

また、MT_Reply_Aメッセージ（２１２Ａ）のSecurity_Field（３１０）は、メッセージ全体を完全に保護するために使用され、移動端末（１０１）とホーム・ネットワーク・オーソライザ（１０３）との間のセ

キュリティの関連付けが使用される。なお、ここでは、MT_Request_Aメッセージ（２０２Ａ）のものと同一のアルゴリズムを使用すべきである。

MT_Reply_Aメッセージ（２１２Ａ）を受け取った後、移動端末（１０１）はすべての必要な情報を検索して、それに従って構成を行い、この設定を使用して、実際のサービス・セッション（２１３）を開始することが可能となる。

実際には、移動端末（１０１）は、例えば、ビデオストリーミング・セッションと一緒にVoice-over-IPセッションを行うなど、いくつかのサービスを同時に要求することが可能である。すなわち、シグナリング内に、異なるサービス・プロバイダ・ネットワークを関係付けることが可能である。同一のメッセージ内にいくつかのサービスの要求をまとめるシナリオにおいて、上記と同一のメカニズム及びメッセージの構造を使用することが可能である。例えば、MT_Request_Aメッセージ（２０２Ａ）内に、Service_Requestフィールド（３０５）、Session_IDフィールド（３０６）、Address_Requestフィールド（３０７）、Tunnel_Requestフィールド（３０８）の複数のセットを存在させることが可能である。これらの４つのフィールドはグループ化され、移動端末（１０１）によって要求された各サービスは、これらの４つのフィールドの１グループを含んでいる。 例えば、MT_Request_Aメッセージ（２０２Ａ）がVoice-over-IPセッション及びビデオストリーミング・セッションを要求した場合には、列挙された４つのフィールドのグループが２つ存在する。

MT_Request_Aメッセージ（２０２Ａ）と同じ内容を含んでいるMT_Request_Bメッセージ（２０２Ｂ）を受け取った後、ホーム・ネットワーク・オーソライザ（１０３）は、移動端末（１０１）によって要求される１つの特定のサービスに対応した、これらの４つのフィールド

の各セットから情報を検索する。ホーム・ネットワーク・オーソライザ（１０３）は、単一のサービスの要求に対して、上記のように要求されたサービスの各々のためのシグナリングを実行する。例えば、ホーム・ネットワーク・オーソライザ（１０３）は、ＩＭＳサブシステム及びストリーミング・サービスを提供するネットワークの両方に、Service_Requestメッセージ（２０３）を送る。また、異なる各サービスに係るWLAN_Requestメッセージ（２０６）が、同一のＷＬＡＮに送られる。ホーム・ネットワーク・オーソライザ（１０３）は情報を集め、ただ１つのメッセージを送ることが可能である。同一のＷＬＡＮに多数のWLAN_Requestメッセージ（２０６）を送る必要がある場合には、それらのうちの１つだけが、ローカルのアドレスの割り付けの要求を行う必要がある。

ホーム・ネットワーク・オーソライザ（１０３）は要求されたサービスの順序に従って、１つのMT_Reply_Bメッセージ（２１２Ｂ）にすべてのサービス情報を統合し、アクセス・ポイント（１０５）を介して、移動端末（１０１）に転送する。その後、移動端末（１０１）は統合されたMT_Reply_Aメッセージ（２１２Ａ）内の情報を用いて、それ自体のアドレス構成を行うことが可能となる。

なお、移動端末（１０１）が並行して多数のサービスを要求した場合には、異なるサービス・プロバイダ・ネットワークからその端末に異なるアドレスが割り当てられる可能性があり、さらに、異なるサービス・セッションにおいて異なるトンネルが設定される可能性がある。このシナリオでは、特別な中間層プロセッサ（mid-layer processer）が必要となる。Session_IDフィールド（３０６）で使用されるようなサービス・セッション識別子が、中間層プロセッサによって使用されて、アドレス及びトンネルの設定が多重化される。

移動端末（１０１）内の中間層プロセッサは、異なるサービス・セッションにおけるアドレス及びトンネル情報のローカルのデータベースを保持している。サービス・セッションが移動端末（１０１）で生成された場合、中間層プロセッサはそのための識別子を作成する。これは、MT_Request_Aメッセージ（２０２Ａ）のSession_IDフィールド（３０６）内で使用されるセッション識別子である。アドレス及びトンネル情報をすべて含むMT_Reply_Aメッセージ（２１２Ａ）を受け取った後、中間層プロセッサは、セッション識別子によって指標化（インデックス化）されたすべての情報を含むデータベース内に、新しいエントリを作成する。サービス・アプリケーションが、新しい接続セッションを開始する必要がある場合には、中間層プロセッサに対してセッション識別子が設定されたリクエストを送り、中間層プロセッサは、このセッション識別子を用いて、データベースから、対応するアドレス及びトンネル情報を検索する。アドレス及びトンネル情報は、例えば、ＩＰレイヤなどの通常のスタックによって使用され、接続を行うために、ソケットなどの適切なバインディングが作られる。

なお、実際には、例えば、ＷＬＡＮサーバ（１０２）などのようなコントローラのないＷＬＡＮが存在可能であることは、当業者にとっては明白である。このような場合には、移動端末（１０１）はアドレスの割り付け及びトンネルの設定のために、ＷＬＡＮのローカルのメカニズムを使用しなくてはならない。ホーム・ネットワーク・オーソライザ（１０３）は、MT_Reply_Aメッセージ（２１２Ａ）内のAddress_Requestフィールド（３０７）及びTunnel_Requestフィールド（３０８）をすべて０にセットし、これによって、移動端末（１０１）に対して、例えば、ＤＨＣＰｖ６、ＭＩＰｖ６などのＷＬＡＮメカニズムを使用してアドレス構成を行うよう強いることになる。

また、ある場合では、移動端末（１０１）が、ＷＬＡＮ内のサービス登録の取り消しを望むことがある。サービスの登録抹消を行う場合でも上記のメカニズムを使用することが可能であることは、当業者にとっては明白である。移動端末（１０１）は、サービスの終了を示す特別の値がService_Requestフィールド（３０５）に設定されたMT_Request_Aメッセージ（２０２Ａ）を送出することが可能である。例えば、Service_Requestフィールド（３０５）は「terminate.request.IMS.foo.bar.operator-name.operatorgroup.gprs」のような値を含むことが可能である。なお、「request（要求）」キーワードの前の「terminate（終了）」が、「request（要求）」キーワードの後に付けられているＡＰＮによって示されたサービスを終了するためのフラグである。また、MT_Request_Aメッセージ（２０２Ａ）のSession_IDフィールド（３０６）は、終了するサービスのセッション識別子に設定可能であり、このタイプのMT_Request_Aメッセージ（２０２Ａ）では、Address_Requestフィールド（３０７）及びTunnel_Requestフィールド（３０８）を省略することが可能である。

ホーム・ネットワーク・オーソライザ（１０３）は、通常と同様に、MT_Request_Aメッセージ（２０２Ａ）の処理を行い、そのService_Requestフィールド（３０５）内に「終了」のキーワードを見つけた場合には、Session_IDフィールド（３０６）からサービス・セッション識別子を取り出す。そして、ホーム・ネットワーク・オーソライザ（１０３）は、サービス登録時に作られたセッション・エントリを探すため、そのデータベースを探索する。このセッション・エントリは、例えば、割り当てられたアドレス、トンネル設定などのサービスの設定に関する情報を格納している。この情報を用いて、通常と同様に、ホーム・ネットワーク・オーソライザ（１０３）は、サービス・プロバイダ

・ネットワーク・サーバ（１０４）にService_Requestメッセージ（２０３）を送り、ＷＬＡＮサーバ（１０２）にWLAN_Requestメッセージ（２０６）を送る。これらのメッセージにおいて、Service_Specフィールド（７０５）及びService_Supportフィールド（８０４）は、すべて０にセットされる。

サービス・プロバイダ・ネットワーク・サーバ（１０４）とＷＬＡＮサーバ（１０２）は、通常通り、メッセージを処理し、Service_Specフィールド（７０５）及びService_Supportフィールド（８０４）がすべて０に設定されているのを読んで、サービス終了の要求であることを把握する。これらの２つのサーバは、サービス登録時に作られたサービス・セッション・エントリを探すため、それらのデータベースを検索し、例えば、ＩＰアドレスや予約している帯域幅などのサービス・セッションに対応するリソースを解放する。

ホーム・ネットワーク・オーソライザ（１０３）が、サービス・プロバイダ・ネットワーク（１００３）及びＷＬＡＮから通知を受け取った後、MT_Reply_Aメッセージ（２１２Ａ）が、移動端末（１０１）に返される。このメッセージは、サービスを終了し、予約されていたリソースが解放されたことを通知するものである。このMT_Reply_Aメッセージ（２１２Ａ）では、Service_Requestフィールド（３０５）に、その結果に関する情報が含まれている。例えば、このフィールドにおいて、次の値「removed.request.IMS.foo.bar.operator-name.operator-group.gprs」を使用することが可能である。ここでは、「request」キーワードの前の「removed」キーワードが、サービスの登録抹消の成功を示している。なお、例えば、「removed」キーワードの後に情報を付加するなど、特別な情報を含めてもよいことは、当業者にとっては明白である。

また、移動端末（１０１）へのサービス提供の過程において、ポリシ

ー・コントロールを含ませることも可能である。例えば、ＧＰＲＳインターフェースを使用する端末は、１４９Ｋｂｐｓのアクセス・レートが与えられている。この端末がＷＬＡＮに入った場合、その端末は、同じサービスにアクセスするためにＷＬＡＮインターフェースを使用するよう移行する。ＷＬＡＮは、はるかに高いエア・インターフェース帯域幅を提供するので、端末がより高いアクセス・レート（例えば、１Ｍｂｐｓ）を享受することを切望する。移動端末（１０１）に対して、このより高いサービス・レートを与えるためには、ポリシー・コントロール・フレームワークが起動され、例えば、ゲートウェイ・フィルタなど、対応するポリシー設定を修正する必要がある。上記の例では、例えば、ＧＧＳＮなどの制御点が、ＧＰＲＳインターフェースを使用してサービスを始める場合には、ＧＧＳＮは、端末のサービスのために１４９Ｋｂｐｓの帯域幅のみを予約すればよい。また、移動端末（１０１）が、再びＷＬＡＮサービスを利用して、サービス・セッションを登録する場合、ポリシー・サーバは、ＧＧＳＮの設定を１Ｍｂｐｓに修正すべきである。なお、他の種類の設定やコントロール・ノードがポリシー・コントロールに含まれることは、当業者にとっては明白である。

この種のポリシー・コントロールは、ユーザの加入情報に従って行われるべきであり、したがって、ホーム・ネットワーク・ドメイン内で行われるべきである。本発明は、サービスの要求及びアドレス（トンネルの設定）を扱うためにホーム・ネットワーク・オーソライザ（１０３）を使用するものである。したがって、それは、ポリシー・コントロール決定のために必要な情報をすべて有しており、ホーム・ネットワーク・ドメインのポリシー・サーバにホーム・ネットワーク・オーソライザ（１０３）から、こうした情報を渡すことが可能である。ポリシー・サーバは、このとき、例えば、ＧＧＳＮなどのコレスポンディング・ノード

を適宜動作させるよう操作可能とするポリシー・コントロール・インターフェースを利用することが可能である。さらに、ポリシー・サーバは、ポリシー・コントロール・フレームワークを使ったサービス提供に関連する他のネットワークに通知を行うことも可能であり、例えば、ホーム・ネットワーク・ドメインのポリシー・サーバは、ＷＬＡＮ内のポリシー・サーバに対して、新しいアクセス・レートの制限を通知することが可能であり、その結果、ＷＬＡＮポリシー・サーバは、ローカルの承認管理機構を適宜調節することが可能となる。

また、図９は、ホーム・ネットワーク・オーソライザ（１０３）とポリシー・サーバとの間で使用されるメッセージの実施例を示すものである。このメッセージは、Operationフィールド（９０１）から始まる。このフィールドは、ポリシー・サーバによって行われる動作を示すものであり、可能な値は次の通りである。

Install::=0x01

Remove::=0x02

Update::=0x03

ホーム・ネットワーク・オーソライザ（１０３）が移動端末（１０１）から新しいサービス・セッションの要求を受け取った場合、Operationフィールド（９０１）内に「Install」の値を使用する。また、移動端末（１０１）がサービス・セッションを終了する場合には、ホーム・ネットワーク・オーソライザ（１０３）は、Operationフィールド（９０１）内に「Removed」の値を使用する。また、移動端末（１０１）からのサービスの要求がアクティブなサービス・セッションを参照している場合には、「Update」の値を使用する。なお、実際の実施においては、他のタイプの値の使用が可能であることは、当業者にとっては明白である。

また、２番目のフィールドは、MT_IDフィールド（９０２）である。

このフィールドは、移動端末（１０１）の識別子を含んでおり、例えば、モバイルのユーザのＩＭＳＩが使用可能である。

また、３番目のフィールドは、MT_Locationフィールド（９０３）である。このフィールドは、例えば、端末が所定のＷＬＡＮに存在する場合には、２倍のアクセス・レートを提供するなど、位置に基づくサービスのポリシーを検索するために、ポリシー・サーバによって使用されるものである。このフィールドは、例えば、MT_Request_Aメッセージ（２０２Ａ）のWLAN_IDフィールド（３０９）からのＷＬＡＮ識別子を含むものである。

また、次のフィールドは、MT_Serviceフィールド（９０４）である。このフィールドは、移動端末（１０１）によって、どのような種類のサービスがアクセスされているかを示すものである。さらに、このフィールドが、サービス・セッション情報を含むことも可能である。このフィールドの内容の例としては、ＡＰＮにセッション識別子を加えたものが可能である。

また、次のフィールドは、Tunnel_Settingフィールド（９０５）である。このフィールドは、ＷＬＡＮ内で移動端末（１０１）によって使用されるトンネルの設定を示すものである。このフィールドの内容はトンネルのタイプであり、トンネルの終端点アドレス、ポート番号などが後続する。なお、正確なフォーマットは、トンネルのタイプに依存する。また、使用されるトンネルのタイプは、MT_Request_Aメッセージ（２０２Ａ）のTunnel_Requestフィールド（３０８）で定義されたものである。

また、メッセージの最後のフィールドは、MT_Addressフィールド（９０６）である。このフィールドは、ＷＬＡＮ内で移動端末（１０１）によって使用されるアドレスを含むものである。これは、ポリシー・サ

ーバによって使用され、サービスにアクセスするフィルタリングの規則を設定することが可能となる。

なお、実際には、メッセージ・フィールドが上記ほど正確な順序で並べられる必要がないことは、当業者にとっては明白である。また、各フィールドは、さらに、本実施例に記述されない他の情報を含むことが可能である。

産業上の利用可能性

本発明は、ＷＬＡＮ相互接続において、端末のアドレス割り当てを管理する管理方法を提供する。本発明の適用によって、移動端末には、それが要求したサービスとその加入情報に基づいてアドレスの割り当てが行われ、ローカル・リソースへのアクセスを必要とせずに、アドレス管理が実行可能となる。さらに、本発明は、ＷＬＡＮ相互接続におけるトンネルの設定のコントロール方法を提供する。ここでは、移動端末は、サービス許可と同時にネットワーク及びクライアントに基づくトンネルの設定をサポートすることができる。さらに、本発明は、ポリシー・コントロール・フレームワークでの相互接続の方法を提供する。提供されるインターフェースを用いることによって、サービス許可、アドレス割り当て、及び、トンネル設定情報をポリシー・サーバに伝播することが可能となり、よりよく端末にサービスを配信するために適切な動作を行うことが可能となる。すべての方法において、端末とそのホーム・ドメイン・サーバとの１回の往復メッセージの交換で、アドレス管理、トンネルの設定及びサービスの許可を達成することが可能である。したがって、貴重なシグナリングの時間や帯域幅が節約される。

請 求 の 範 囲

1． 移動端末と、前記移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラとの間におけるセキュリティ保護された終端点間サービス許可シグナリングをアドレスの管理のために利用することによって、前記コントローラがサービス許可情報に基づくアドレス割り当ての管理を行うことが可能であり、ローカルＷＬＡＮアクセス制御に基づくことなく、ＷＬＡＮ相互接続において前記移動端末のアドレス割り当ての管理を行うためのシステム。

2． 移動端末と、前記移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラとの間におけるセキュリティ保護された終端点間サービス許可シグナリングをトンネルの管理のために利用することによって、前記コントローラがサービス許可情報に基づくトンネル管理を行うことが可能であり、ローカルＷＬＡＮアクセス制御に基づくことなく、ＷＬＡＮ相互接続において前記移動端末のトンネルの管理を行うためのシステム。

3． 移動端末と、前記移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラとの間におけるセキュリティ保護された終端点間サービス許可シグナリングをアドレス及びトンネルの管理のために利用することによって、前記コントローラがサービス許可情報に基づくアドレス割り当て及びトンネルの管理を行うことが可能であり、ローカルＷＬＡＮアクセス制御に基づくことなく、ＷＬＡＮ相互接続において前記移動端末のアドレス

割り当て及びトンネルの管理を行うためのシステム。

４．　前記ローカルＷＬＡＮアクセス制御処理に由来したシグナリング・メッセージの保護及び暗号化のためのセキュリティ連携を利用することによって、前記ＷＬＡＮ相互接続の前記シグナリング・メッセージを保護するよう構成されている請求項１から３のいずれか１つに記載のシステム。

５．　前記移動端末のドメイン情報を利用することによって、前記移動端末のホーム・ドメイン内の前記コントローラの位置情報を特定するよう構成されている請求項１から３のいずれか１つに記載のシステム。

６．　前記移動端末がそのドメイン情報をメッセージ内に埋め込み、前記移動端末と前記コントローラとの間に存在する中間ノードが前記ドメイン情報を参照して、前記ドメイン情報に基づいて前記メッセージを転送することによって、前記中間ノードが、前記コントローラに前記メッセージを転送するためのアドレスを決定するよう構成されている請求項１から３のいずれか１つに記載のシステム。

７．　ｉ．　アドレス割り当て要求及びアドレス割り当て応答に、所定のワイルドカード値を使用することによって、前記移動端末におけるステートレスなアドレス構成をサポートし、

ｉｉ．　前記アドレス割り当て要求及び前記アドレス割り当て応答に、アドレスのタイプのリストを入れることによって、前記移動端末におけるアドレスの異なるタイプをサポートし、

ｉｉｉ．　アドレス管理情報にアドレスのプリフィックスを入れることに

よって、前記移動端末に対する複数のアドレスの割り当てをサポートするよう構成されている請求項１又は３に記載のシステム。

８．　ｉ．　前記移動端末が、前記サービス・アクセス・セッションを一意に識別する識別子を生成し、

ii．　前記移動端末と前記コントローラとの間のアドレスに係るメッセージに、前記サービス・アクセス・セッションの識別子を入れることによって、アドレス割り当て処理と前記サービス・アクセス・セッションとの関連付けを行い、

iii．　前記コントローラが、前記移動端末の前記サービス・アクセス・セッションで利用される前記アドレスをトレースし、

iv．　前記コントローラが、前記サービス・アクセス・セッションの識別子を利用して、前記サービス・アクセス・セッションにおいて前記移動端末によって使用されるアドレスを検索するよう構成されている請求項１又は３に記載のシステム。

９．　前記コントローラが、前記サービス・アクセス・セッションで使用される前記移動端末のアドレスの格納管理を行うためのバックエンド・サーバを利用するよう構成されている請求項８に記載のシステム。

１０．　前記コントローラは、

ｉ．　前記移動端末の識別子と前記サービス・アクセス・セッションの識別子とを指標とするエントリが前記コントローラのレコード内に存在しない場合には、前記移動端末の識別子と、前記サービス・アクセス・セッションの識別子とを指標とする新たなエントリを作成し、

ii．　前記サービス・アクセス・セッション用に前記移動端末に割り

当てる前記アドレスが設定された前記エントリを格納し、

iii. 前記移動端末が前記サービス・アクセス・セッションを終了した場合には、格納されている前記エントリを削除して、

前記コントローラが、前記ＷＬＡＮ相互接続における前記移動端末の前記アドレス構成を保持するよう構成されている請求項８に記載のシステム。

１１. i. サービス許可メッセージにおいて、アドレス割り当て要求とそれに対応するサービス・アクセス要求とをグループ化することによって、複数の異なるサービス・アクセス・セッションに対する複数のアドレスの割り当てをサポートし、

ii. 前記コントローラが、前記移動端末の異なるサービス・アクセス要求に基づいて、異なるアドレス構成を取得して、

前記移動端末における同時サービス・セッションが可能となるよう構成されている請求項１又は３に記載のシステム。

１２. i. 前記移動端末が、対応する前記アドレス構成と共に前記サービス・アクセス・セッション情報を格納するためのローカルデータベースを保持し、

ii. サービス・アクセス・セッションの識別子を使用して、アドレスを多重化することによって、前記移動端末が、異なるサービスにアクセスするために異なるアドレスを使用して、

複数のサービス・セッションに対する複数のアドレス構成をサポートするよう構成されている請求項１１に記載のシステム。

１３. i. 前記ポリシー・サーバとのインターフェースを設定

することによって、前記コントローラが、前記移動端末にサービスを提供するためのポリシー構成を修正できるようにし、

ii． ＷＬＡＮ内の前記移動端末にサービスを提供するためのコントロール・ノードに対するポリシー・コントロール・フレームワークを通じたポリシー・シグナリングを、前記コントローラに開始させることによって、前記コントロール・ノードに関するポリシー設定を適応させて、

ポリシー設定の調整が可能となるよう構成されている請求項１から３のいずれか１つに記載のシステム。

１４． 前記サービスの許可を行うサービス・オーソライザと、前記ポリシー・サーバとの間の情報交換に利用されるメッセージのフォーマットが、

i． 前記ポリシー・サーバで行われる動作を示すオペレーション識別子部と、

ii． 前記移動端末の識別子を含む移動端末識別子部と、

iii． 前記移動端末に対して、前記移動端末の位置に基づくポリシーを適用するための前記移動端末の位置情報を含む移動端末位置情報部と、

iv． 前記サービスのタイプと、必要に応じて前記サービスのセッション識別子とを含む移動端末サービス情報部と、

v． 前記サービスにアクセスするために、前記移動端末によって利用されるトンネル設定情報を含むトンネル設定情報部と、

vi． 前記サービスにアクセスするための前記移動端末の前記アドレスを含むアドレス情報部とを、

有する請求項１３に記載のシステム。

１５． i． 移動端末のユーザ加入情報にアクセス可能であり、

前記移動端末のホーム・ドメイン内に配置されているコントローラに対して、前記移動端末が、セキュリティ保護された終端点間のサービス許可要求と共に、アドレス管理要求を送信するステップと、

ii. 前記コントローラが、前記サービス許可要求及び前記ユーザ加入情報に基づいて、前記移動端末が前記サービスへのアクセスを行うためのアドレスを割り当てるステップと、

iii. 前記コントローラが、セキュリティ保護された終端点間サービス許可シグナリングを用いて、アドレス管理情報を前記移動端末に送信するステップとを、

有し、ローカルＷＬＡＮアクセス制御に基づくことなく、ＷＬＡＮ相互接続において前記移動端末が前記サービスにアクセスするためのアドレス割り当ての管理を行うための方法。

１６. i. 移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラに対して、前記移動端末が、セキュリティ保護された終端点間のサービス許可要求と共に、トンネル管理要求を送信するステップと、

ii. 前記コントローラが、前記サービス許可要求及び前記ユーザ加入情報に基づいて、前記移動端末が前記サービスへのアクセスを行うためのトンネル構成を決定するステップと、

iii. 前記コントローラが、セキュリティ保護された終端点間サービス許可シグナリングを用いて、前記トンネル構成情報を前記移動端末に送信するステップとを、

有し、ローカルＷＬＡＮアクセス制御に基づくことなく、ＷＬＡＮ相互接続において前記移動端末が前記サービスにアクセスするためのトンネルの管理を行うための方法。

１７．　　ｉ．　移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラに対して、前記移動端末が、セキュリティ保護された終端点間のサービス許可要求と共に、アドレス及びトンネル管理要求を送信するステップと、

ｉｉ．　前記コントローラが、前記サービス許可要求及び前記ユーザ加入情報に基づいて、前記移動端末が前記サービスへのアクセスを行うためのアドレス及びトンネル構成を決定するステップと、

ｉｉｉ．　前記コントローラが、セキュリティ保護された終端点間サービス許可シグナリングを用いて、前記アドレス及び前記トンネル構成に係る情報を前記移動端末に送信するステップとを、

有し、ローカルＷＬＡＮアクセス制御に基づくことなく、ＷＬＡＮ相互接続において前記移動端末が前記サービスにアクセスするためのアドレス割り当て及びトンネルの管理を行うための方法。

１８．　　前記ローカルＷＬＡＮアクセス制御処理に由来したシグナリング・メッセージの保護及び暗号化のためのセキュリティ連携を利用することによって、前記ＷＬＡＮ相互接続の前記シグナリング・メッセージを保護する請求項１５から１７のいずれか１つに記載の方法。

１９．　　前記移動端末のドメイン情報を利用することによって、前記移動端末のホーム・ドメイン内の前記コントローラの位置情報を特定する請求項１５から１７のいずれか１つに記載の方法。

２０．　　前記移動端末がそのドメイン情報をメッセージ内に埋め込み、前記移動端末と前記コントローラとの間に存在する中間ノードが前

記ドメイン情報を参照して、前記ドメイン情報に基づいて前記メッセージを転送することによって、前記中間ノードが、前記コントローラに前記メッセージを転送するためのアドレスを決定する請求項１５から１７のいずれか１つに記載の方法。

２１．　前記移動端末によって要求される前記サービスを提供するネットワーク内のアドレス管理エンティティと前記コントローラとの間で、前記移動端末による前記サービスへのアクセスに利用されるアドレスの交渉を行うステップをさらに有する請求項１５に記載の方法。

２２．　ｉ．　前記移動端末が、前記コントローラに対して送信するアドレス割り当て要求に、特定のアドレスを入れるステップと、

ii．　前記移動端末からの前記アドレス割り当て要求と、前記移動端末によりアクセスされるサービスに係る情報とに従って、使用される前記アドレスを前記移動端末に割り当てるステップとを、

有し、前記移動端末におけるサービス中断を抑制する請求項１５に記載の方法。

２３．　ｉ．　前記移動端末が、前記トンネル要求メッセージに、前記トンネルのタイプのリストを入れるステップと、

ii．　前記移動端末及びコントローラが、前記トンネル要求メッセージ及びトンネル構成メッセージに、トンネルの方向に係る情報を入れるステップとを、

有し、複数のトンネルのタイプ及び方向をサポートする請求項１６又は１７に記載の方法。

２４．　前記移動端末によって要求される前記サービスを提供するネットワーク内の実際のトンネル終端点と前記コントローラとの間で、前記移動端末による前記サービスへのアクセスに利用されるトンネル構成の交渉を行うステップをさらに有し、前記移動端末の前記トンネル構成の管理を行う請求項１６又は１７に記載の方法。

２５．　ｉ．　前記コントローラが、前記移動端末による前記サービスへのアクセスに利用されるトンネルを管理する前記ＷＬＡＮ内のトンネル管理エンティティと通信を行うステップと、

ii．　前記ＷＬＡＮ内の前記トンネル管理エンティティが、前記コントローラとの通信結果に応じて、前記トンネルを使用可又は使用不可とするステップとを、

さらに有し、前記移動端末の前記トンネル構成の管理を行う請求項１６又は１７に記載の方法。

２６．　前記コントローラが、前記ＷＬＡＮ内の前記トンネル終端点の識別及び構成を行うために、前記ＷＬＡＮ内のトンネル管理エンティティと通信を行うステップと、

前記コントローラが、前記移動端末に前記サービスを提供するネットワーク内の前記トンネル終端点の識別及び構成を行うために、前記ネットワーク内のトンネル管理エンティティと通信を行うステップとを、

さらに有し、前記移動端末が前記サービスにアクセスするためのサイト間ネットワーク・トンネルの設定を行う請求項１６又は１７に記載の方法。

２７．　前記コントローラが、前記ユーザ加入情報を参照するため、

前記移動端末のホーム・ネットワーク内のバックエンド・サーバとの通信を行うステップを有する請求項１６又は１７に記載の方法。

２８．　前記移動端末によって使用されるメッセージのフォーマットが、

ｉ．　すべてのネットワーク・ノードがアクセス可能な前記移動端末のホーム・ドメイン情報部と、

ii．　前記サービス要求を許可するノードのみがアクセス可能な前記ユーザの識別情報部と、

iii．　前記サービス要求を許可するノードのみがアクセス可能な１つ以上のサービス許可要求を含むサービス要求情報部と、

iv．　ＷＬＡＮ識別情報部と、

ｖ．　前記サービス要求に対応する１つ以上のアドレス要求を含むアドレス要求情報部とを、

有する請求項１５又は１７に記載の方法。

２９．　前記移動端末によって使用されるメッセージのフォーマットが、

ｉ．　前記移動端末のホーム・ドメインの識別情報部と、

ii．　前記サービス要求を許可するノードのみがアクセス可能な前記ユーザの識別情報部と、

iii．　前記サービス要求を許可するノードのみがアクセス可能な１つ以上のサービス許可要求を含むサービス要求情報部と、

iv．　ＷＬＡＮの識別子を含むＷＬＡＮ識別情報部と、

ｖ．　前記サービス要求に対応する１つ以上のトンネル構成要求を含むトンネル構成要求情報部とを、

有する請求項１６又は１７に記載の方法。

３０．　前記コントローラによって使用されるメッセージのフォーマットが、

ｉ．　前記移動端末のホーム・ネットワークの識別情報部と、

ii．　前記サービスの要求に関するサービス・セッションの識別情報部と、

iii．　前記サービス要求における前記移動端末の識別情報部と、

iv．　１つ以上のサービス要求を含むサービス要求情報部と、

ｖ．　前記サービス要求に対応する１つ以上のアドレス構成要求を含むアドレス構成要求情報部とを、

有する請求項２１に記載の方法。

３１．　前記コントローラによって使用されるメッセージのフォーマットが、

ｉ．　前記移動端末のホーム・ネットワークの識別情報部と、

ii．　前記サービスの要求に関するサービス・セッションの識別情報部と、

iii．　前記サービス要求における前記移動端末の識別情報部と、

iv．　１つ以上のサービス要求を含むサービス要求情報部と、

ｖ．　前記サービス要求に対応する１つ以上のトンネル構成要求を含むトンネル構成要求情報部とを、

有する請求項２４に記載の方法。

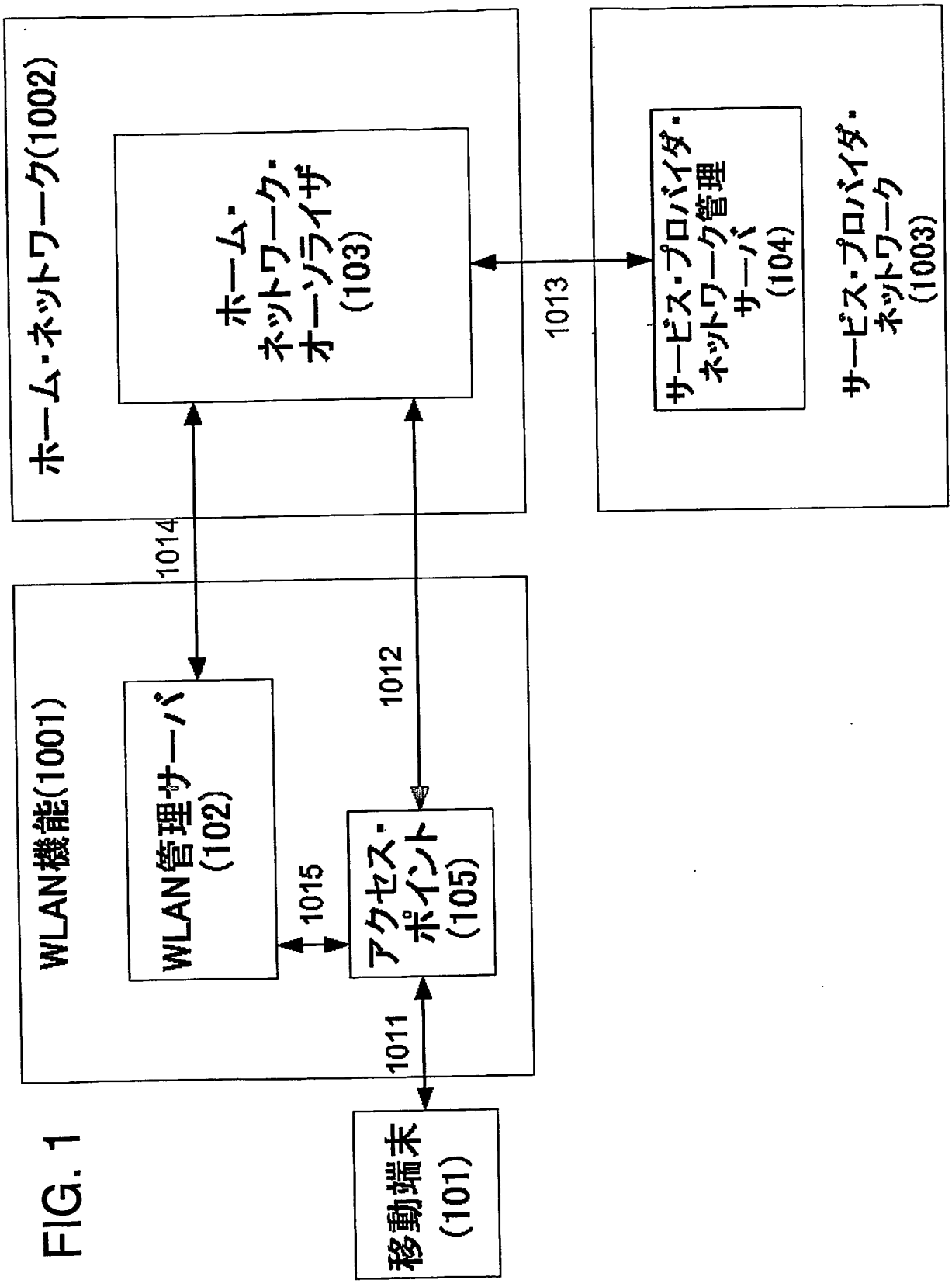

ホーム・ネットワーク(1002)
ホーム・
ネットワーク・
オーソライザ
(103)
1013
サービス・プロバイダ・
ネットワーク管理
サーバ
(104)
サービス・プロバイダ・
ネットワーク
(1003)
1014
WLAN機能(1001)
WLAN管理サーバ
(102)
1012
1015
アクセス・
ポイント
(105)
1011
移動端末
(101)

FIG. 1

FIG. 2

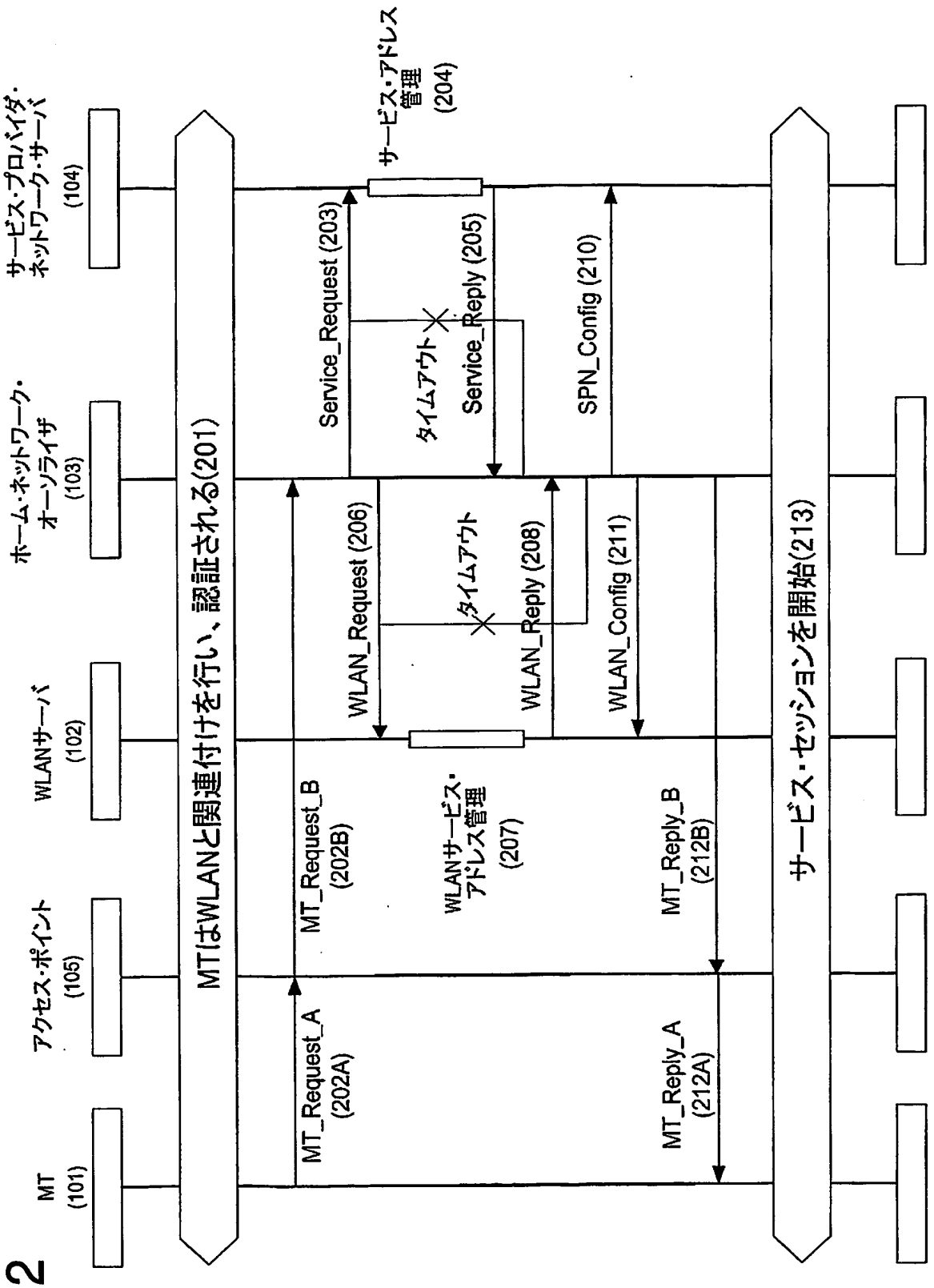

MT (101)
アクセス・ポイント (105)
WLANサーバ (102)
ホーム・ネットワーク・オーソライザ (103)
サービス・プロバイダ・ネットワーク・サーバ (104)
サービス・アドレス管理 (204)
MTはWLANと関連付けを行い、認証される(201)
MT_Request_A (202A)
MT_Request_B (202B)
Service_Request (203)
タイムアウト
Service_Reply (205)
SPN_Config (210)
WLAN_Request (206)
タイムアウト
WLAN_Reply (208)
WLAN_Config (211)
WLANサービス・アドレス管理 (207)
MT_Reply_B (212B)
MT_Reply_A (212A)
サービス・セッションを開始(213)

FIG. 3

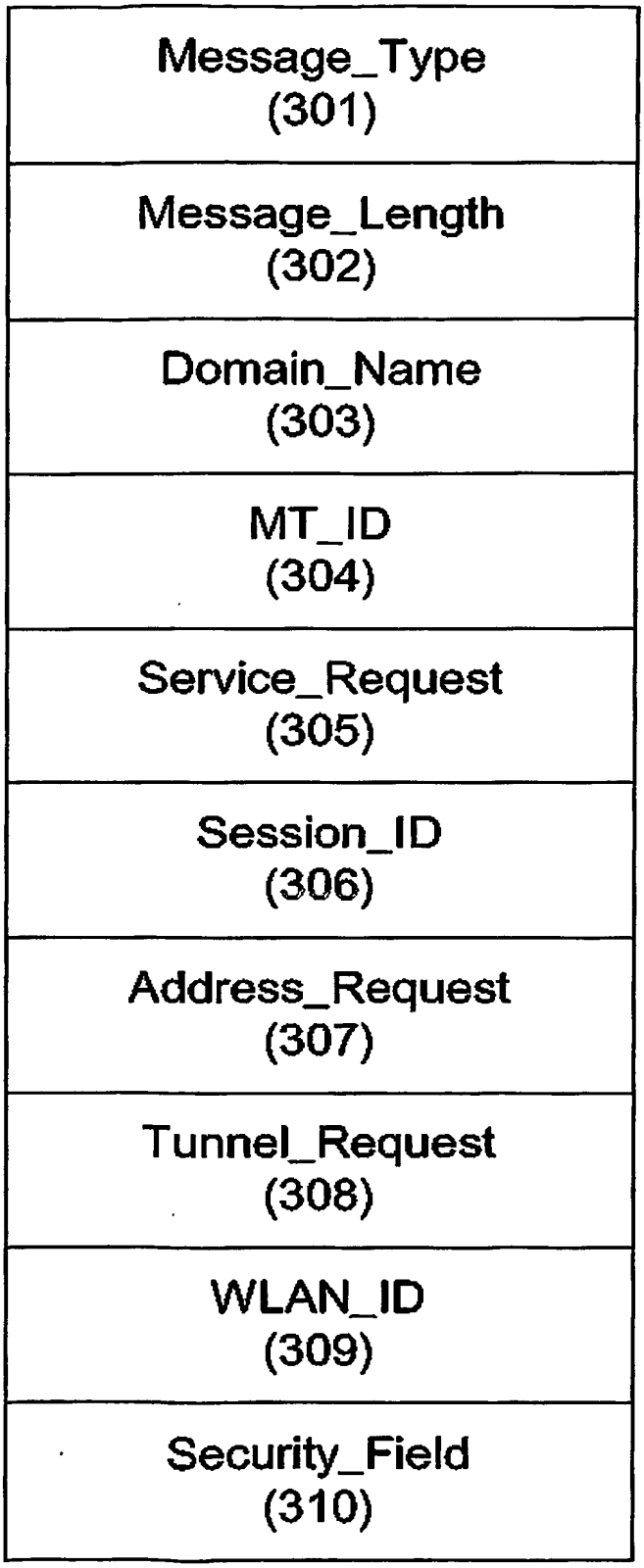

Message_Type
(301)
Message_Length
(302)
Domain_Name
(303)
MT_ID
(304)
Service_Request
(305)
Session_ID
(306)
Address_Request
(307)
Tunnel_Request
(308)
WLAN_ID
(309)
Security_Field
(310)

FIG. 4

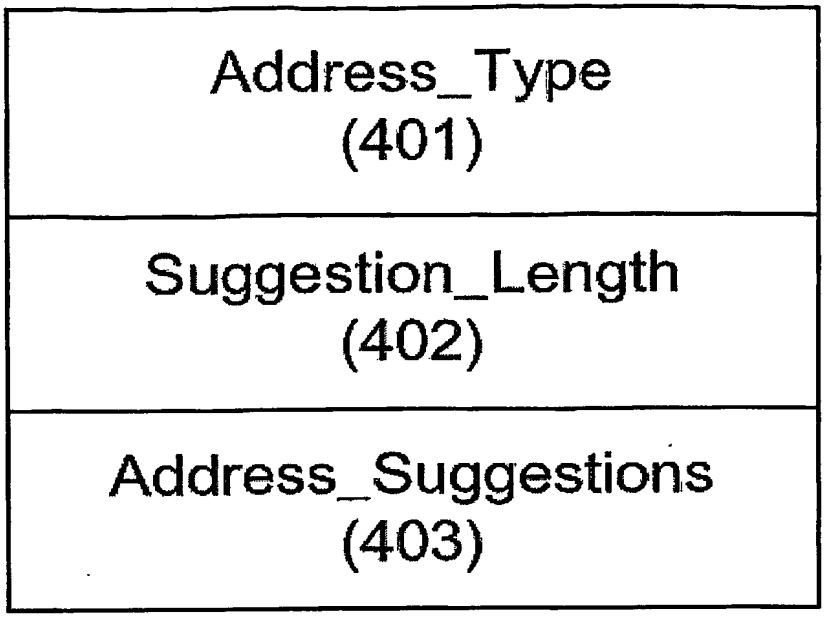

Address_Type
(401)
Suggestion_Length
(402)
Address_Suggestions
(403)

FIG. 5

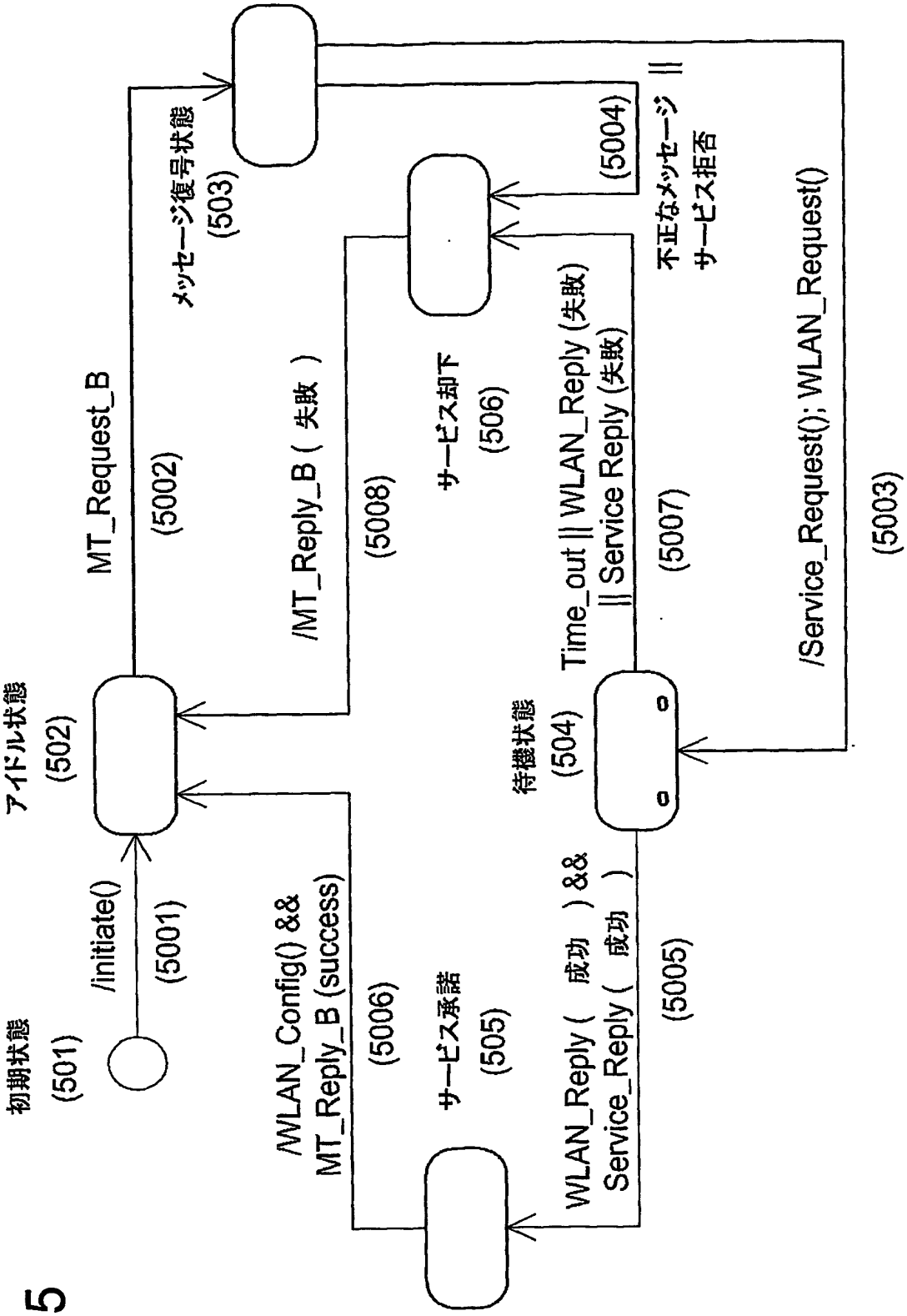

初期状態
(501)
/initiate()
(5001)
アイドル状態
(502)
MT_Request_B
(5002)
メッセージ復号状態
(503)
/Service_Request(); WLAN_Request()
(5003)
WLAN_Reply (成功) &&
Service_Reply (成功)
(5005)
待機状態
(504)
Time_out || WLAN_Reply (失敗)
|| Service Reply (失敗)
(5007)
不正なメッセージ ||
サービス拒否
(5004)
/WLAN_Config() &&
MT_Reply_B (success)
(5006)
サービス承諾
(505)
/MT_Reply_B (失敗)
(5008)
サービス却下
(506)

FIG. 6

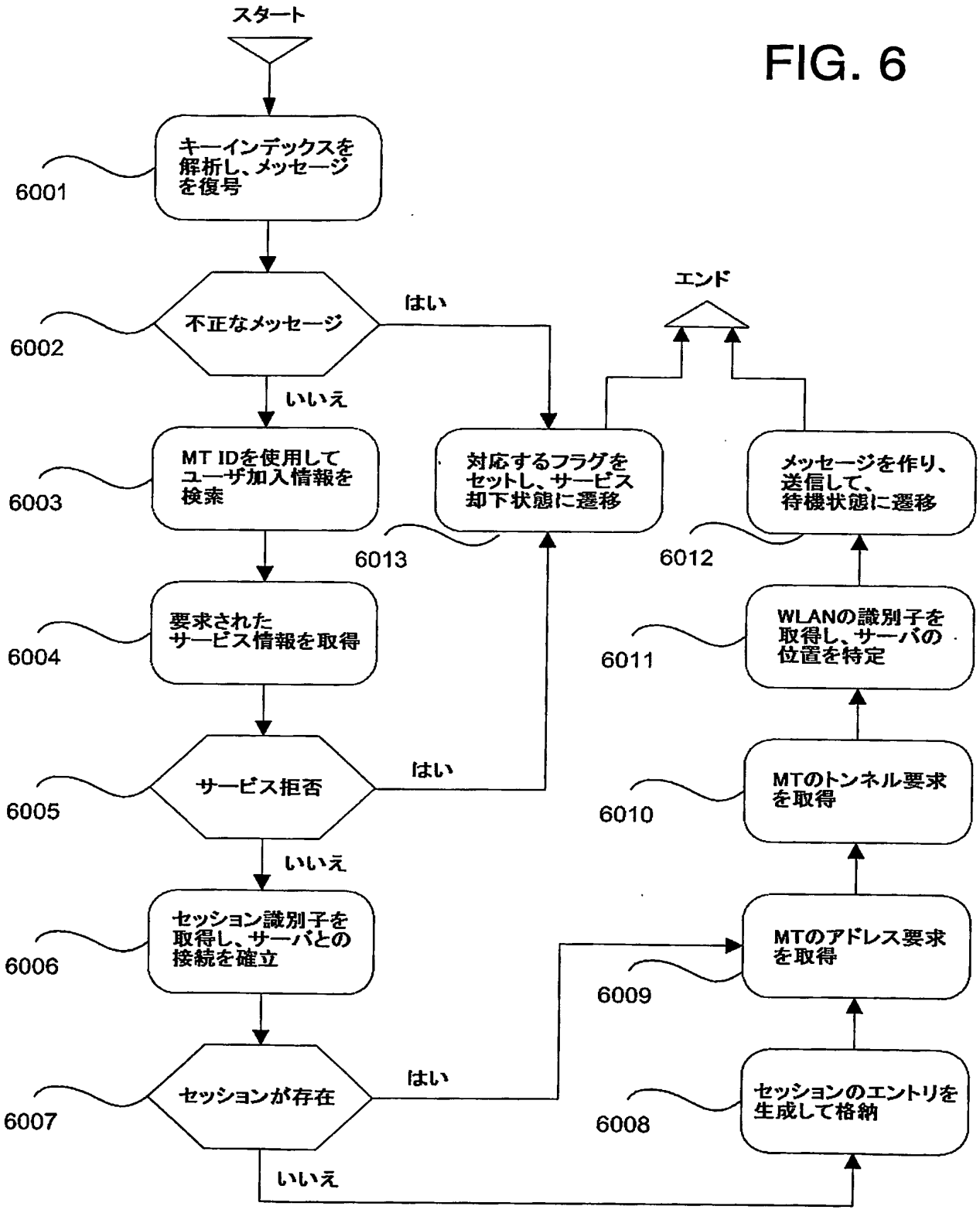

スタート
キーインデックスを解析し、メッセージを復号
6001
不正なメッセージ
6002
はい
いいえ
MT IDを使用してユーザ加入情報を検索
6003
要求されたサービス情報を取得
6004
サービス拒否
6005
はい
いいえ
セッション識別子を取得し、サーバとの接続を確立
6006
セッションが存在
6007
はい
いいえ
対応するフラグをセットし、サービス却下状態に遷移
6013
エンド
メッセージを作り、送信して、待機状態に遷移
6012
WLANの識別子を取得し、サーバの位置を特定
6011
MTのトンネル要求を取得
6010
MTのアドレス要求を取得
6009
セッションのエントリを生成して格納
6008

FIG. 7

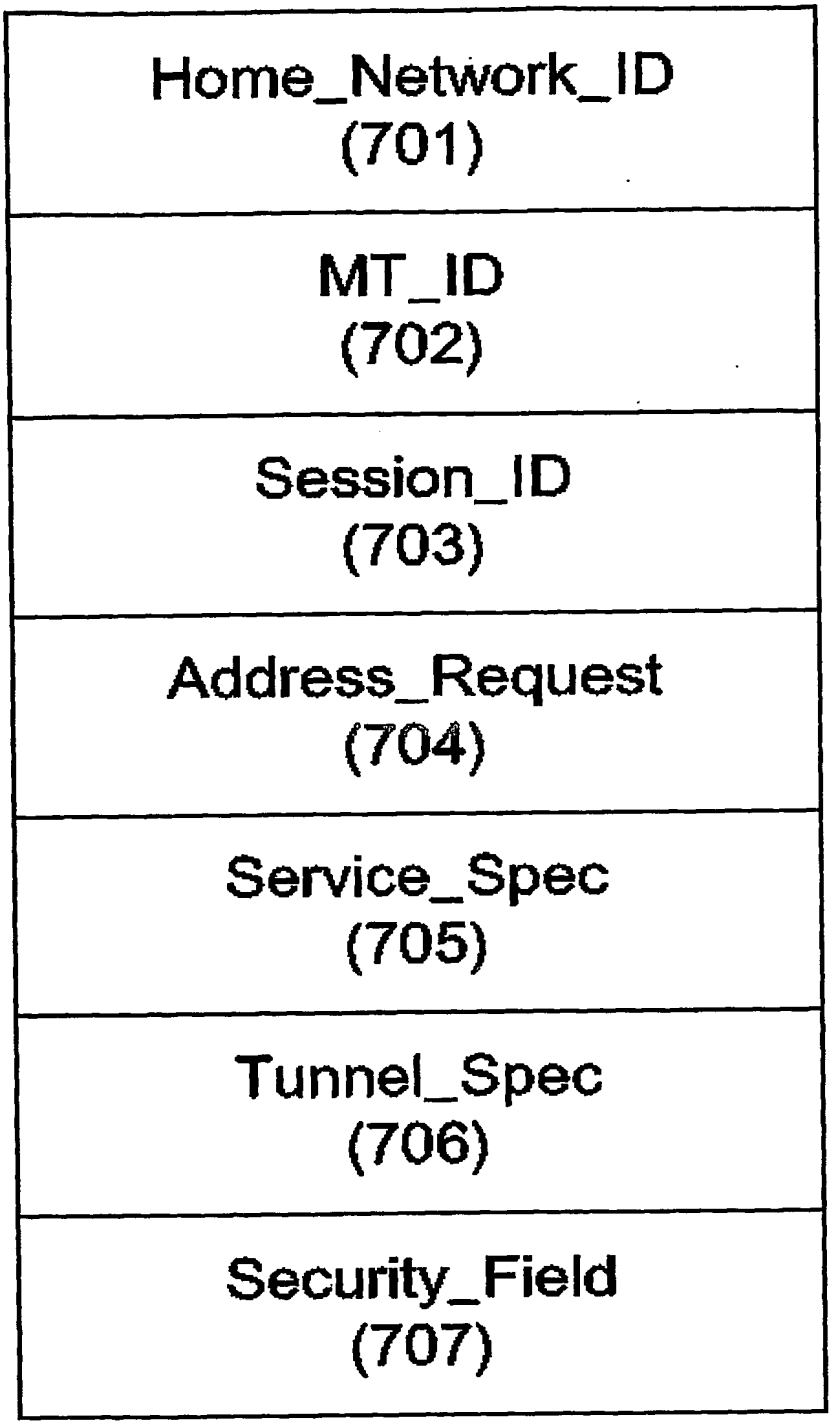

Home_Network_ID
(701)
MT_ID
(702)
Session_ID
(703)
Address_Request
(704)
Service_Spec
(705)
Tunnel_Spec
(706)
Security_Field
(707)

FIG. 8

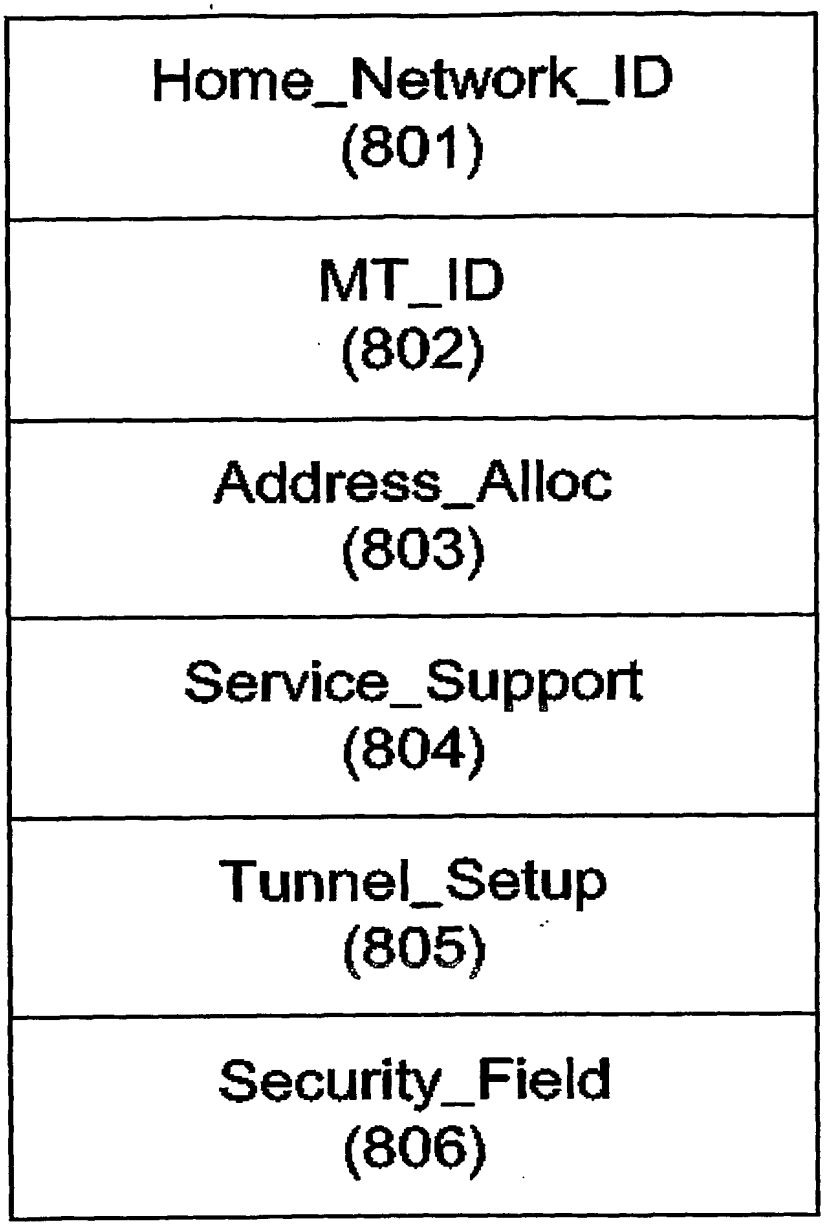
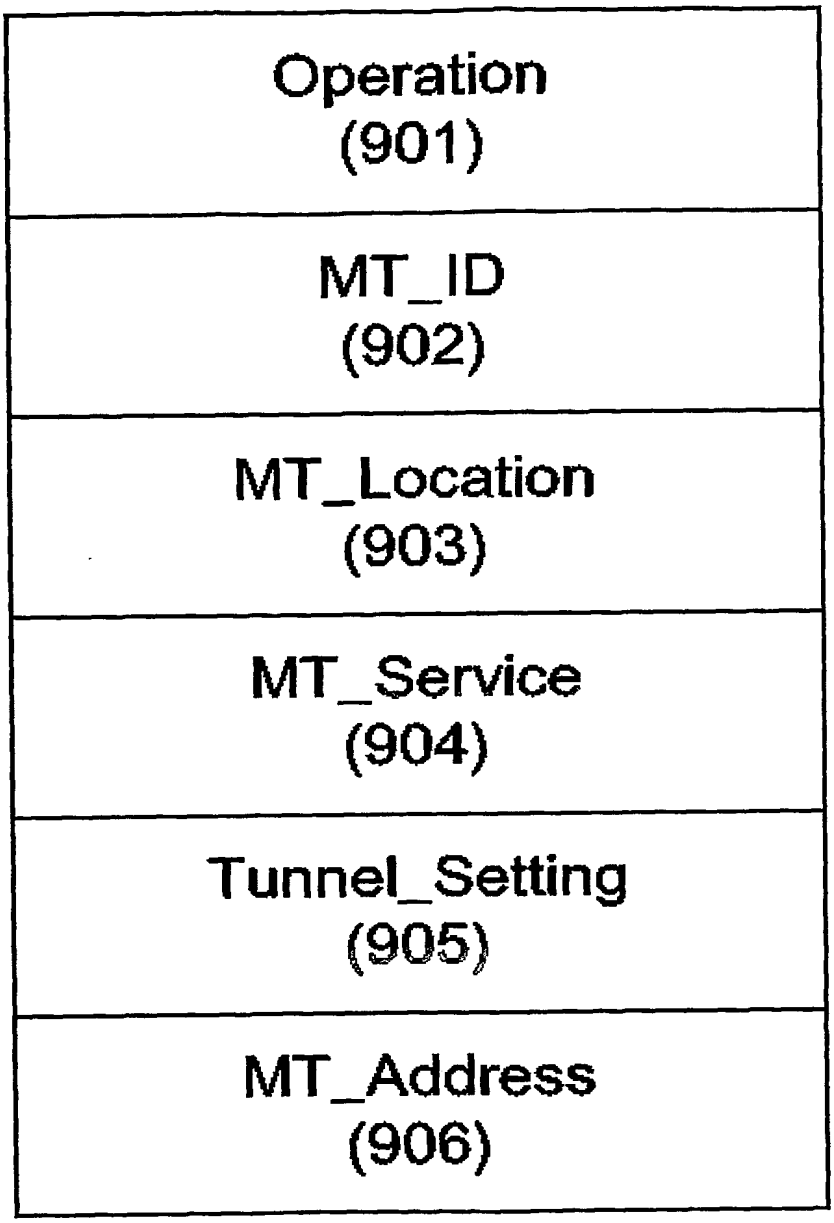

Home_Network_ID
(801)
MT_ID
(802)
Address_Alloc
(803)
Service_Support
(804)
Tunnel_Setup
(805)
Security_Field
(806)

FIG. 9


Operation
(901)
MT_ID
(902)
MT_Location
(903)
MT_Service
(904)
Tunnel_Setting
(905)
MT_Address
(906)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/000176

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/46, H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/00-12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 9-55762 A (Nippon Telegraph And Telephone Corp.), 25 February, 1997 (25.02.97), Full text; Figs. 1 to 5 (Family: none)	1-31
A	JP 10-32610 A (NEC Corp.), 03 February, 1998 (03.02.98), Full text; Figs. 1 to 7 & US 6016318 A	1-31
A	JP 2002-94546 A (KDDI Corp.), 29 March, 2002 (29.03.02), Full text; Figs. 1 to 5 (Family: none)	1-31

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 01 April, 2004 (01.04.04)	Date of mailing of the international search report 13 April, 2004 (13.04.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０００１７６

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ１２／４６
Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ１２／２８

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ１２／００－１２／６６

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６
日本国公開実用新案公報	１９７１－２００４
日本国実用新案登録公報	１９９６－２００４
日本国登録実用新案公報	１９９４－２００１

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　９－５５７６２　Ａ（日本電信電話株式会社）１９９７．０２．２５，全文，図１－５（ファミリーなし）	１－３１
Ａ	ＪＰ　１０－３２６１０　Ａ（日本電気株式会社）１９９８．０２．０３，全文，図１－７　＆　ＵＳ　６０１６３１８　Ａ	１－３１
Ａ	ＪＰ　２００２－９４５４６　Ａ（ケイディーディーアイ株式会社）２００２．０３．２９，全文，図１－５（ファミリーなし）	１－３１

☐ Ｃ欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０１．０４．２００４	国際調査報告の発送日 13.4.2004
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 宮島　郁美　　５Ｘ　８５２３ 電話番号　０３－３５８１－１１０１　内線　３５９５